

S5860 Series Switches CLI Reference Guide

Models: S5860-20SQ; S5860-24XB-U; S5860-48SC

Contents

Ethernet Configuration Commands.....	1
1 Interface Commands.....	1
2 MAC Address Commands.....	34
3 Aggregate Port Commands.....	51
4 VLAN Commands.....	69
5 Super-VLAN Commands.....	79
6 Private VLAN Commands.....	83
7 MSTP Commands.....	92
8 GVRP Commands.....	125
9 LLDP Commands.....	136
10 QinQ Commands.....	167
11 ERPS Commands.....	180
IP Address & Application Commands.....	193
1 IP Address/Service Commands.....	193
2 ARP Commands.....	214
3 IPv6 Commands.....	240
4 DHCP Commands.....	277
5 DHCPv6 Commands.....	322
6 DNS Commands.....	342
7 FTP Server Commands.....	347
8 FTP CLIENT Commands.....	354
9 TFTP Server Commands.....	360
10 TCP Commands.....	363
11 IPv4/IPv6 REF Commands.....	378
Multicast Commands.....	395
1 IPv4 Multicast Routing Configuration Commands.....	395
2 IPv6 Multicast Routing Commands.....	410
3 IGMP Commands.....	423
4 MLD Commands.....	443
5 PIM-DM Commands.....	460
6 PIM-SM Commands.....	473
7 PIM-SMv6 Commands.....	505
8 IGMP Snooping Commands.....	540
9 MLD Snooping Commands.....	566
10 MSDP Commands.....	585
Network Management & Monitoring Commands.....	608
1 SNMP Commands.....	608
2 RMON Commands.....	630
3 NTP Commands.....	640
4 SNTP Commands.....	650
5 SPAN-RSPAN Commands.....	653
6 sFlow Commands.....	659

Reliability Configuration Commands.....	670
1 REUP Commands.....	670
2 RLDLP Commands.....	683
3 VRRP Commands.....	688
4 VRRP Plus Commands.....	707
5 BFD Commands.....	715
6 IP Event Dampening Commands.....	722
7 stacking Commands.....	725
8 RNS &Track Commands.....	748
System Configuration Commands.....	777
1 Command Line Interface Commands.....	777
2 Basic Configuration Management Commands.....	782
3 Line Commands.....	826
4 File System Commands.....	851
5 SYS Commands.....	868
6 Time Range Commands.....	894
7 HTTP Service Commands.....	898
8 Syslog Commands.....	907
9 CWMP Commands.....	949
10 Module Hot-plugging/ unplugging Commands.....	962
11 Supervisor Module Redundancy Commands.....	968
12 Package Management Commands.....	974
13 OpenFlow Commands.....	989
ACL & QoS Configuration Commands.....	994
1 ACL Commands.....	994
2 QoS Commands.....	1045
3 MMU Commands.....	1081
IP Routing Commands.....	1097
1 RIP Commands.....	1097
2 OSPFv2 Commands.....	1138
3 OSPFv3 Commands.....	1230
4 IS-IS Commands.....	1288
5 BGP4 Commands.....	1363
6 PBR Commands.....	1491
7 VRF Commands.....	1516
8 RIPng Commands.....	1527
9 NSM Commands.....	1541
10 Protocol-independent Commands.....	1563
Security Configuration Commands.....	1628
1 AAA Commands.....	1628
2 RADIUS Commands.....	1658
3 TACACS+ Commands.....	1684
4 802.1X Commands.....	1691
5 Web Authentication Commands.....	1737

6 SCC Commands.....	1772
7 Global IP-MAC Binding Commands.....	1778
8 Password-Policy Commands.....	1783
9 Port Security Commands.....	1788
10 Storm Control Commands.....	1801
11 SSH Commands.....	1803
12 URPF Commands.....	1817
13 CPU Protection Commands.....	1824
14 DHCP Snooping Commands.....	1837
15 DHCPv6 Snooping Commands.....	1851
16 ARP-Check Commands.....	1868
17 DAI Commands.....	1870
18 IP Source Guard Commands.....	1874
19 IPv6 Source Guard Commands.....	1879
20 Anti-ARP Spoofing Commands.....	1882
21 NFPP Commands.....	1884
22 DoS Protection Commands.....	1966

Ethernet Configuration Commands

1 Interface Commands

1.1 bandwidth

	Use this command to set the bandwidth on the interface. Use the no form of this command to restore the default setting.	
	bandwidth <i>kilobits</i>	
	no bandwidth	
Parameter Description	Parameter	Description
	<i>kilobits</i>	Bandwidth per second, in the unit of Kbps.
Defaults	If this command is not configured on the interface, use the show interface command to display the default setting in privileged EXEC mode.	
Command Mode	Interface configuration mode	
Usage Guide	This command does not affect the actual bandwidth on the interface. Instead, it is used to display the system the bandwidth specification. By default, the bandwidth is determined by the actual link rate on the interface. It can be set by the user as well.	
Configuration Examples	The following example sets the bandwidth on the interface to 64 Kbps. <pre>FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# bandwidth 64</pre>	
Related	Command	Description
	N/A	N/A
Platform Description	N/A	

1.2 carrier-delay

	Use this command to set the carrier delay on the interface. Use the no form of this command to restore the default value.	
	carrier-delay { [<i>milliseconds</i>] <i>num</i> up [<i>milliseconds</i>] <i>num</i> down [<i>milliseconds</i>] <i>num</i> }	
	no carrier-delay	
Parameter Description	Parameter	Description
	<i>num</i>	(Optional) in the range from 0 to 60 in the unit of seconds.
	<i>milliseconds</i>	(Optional) in the range from 0 to 60000 in the unit of milliseconds.
	up	(Optional) Configures the delay after which DCD changes from Down to Up in status.
	down	(Optional) Configures the delay after which DCD changes from Up to Down in status.
Defaults	The default is 2 seconds.	

Command Mode	Interface configuration mode	
Usage Guide	This parameter refers to the delay after which the carrier detection signal DCD of the interface link changes from the Down status to the Up status or vice versa. If the DCD changes within the delay, the system will ignore such changes without disconnecting the upper data link layer for renegotiation. If the DCD carrier is disconnected for a long time, the parameter should be set longer to accelerate route aggregation so that the routing table can be converged more quickly. On the contrary, if the DCD carrier interruption period is shorter than the time used for route aggregation, you should set the parameter to a higher value to avoid unnecessary route vibration.	
Configuration Examples	The following example sets the carrier delay of serial interface to 5 seconds. <pre>FS(config)# interface gigabitethernet 1/1 FS(config)# carrier-delay 5</pre> The following example sets the carrier delay of serial interface to 100 milliseconds. <pre>FS(config)# interface GigabitEthernet 1/1 FS(config-if-GigabitEthernet 1/1)#carrier-delay milliseconds 100</pre> The following example sets the DCD delay from Down to Up in status to 100 milliseconds and from Up to Down to 200 milliseconds. <pre>FS(config)# interface GigabitEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# carrier-delay up milliseconds 100 down milliseconds 200</pre>	
Related Command	Command	Description
	N/A	N/A
Platform Description	N/A	

1.3 clear counters

	Use this command to clear the counters on the specified interface.	
	clear counters [<i>interface-type interface-number</i>]	
Parameter	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface ID
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	In the privileged EXEC mode, use the show interfaces command to display the counters or the clear counters command to clear the counters. If the interface is not specified, the counters on all interfaces will be cleared.	
Configuration Examples	The following example clears the counters on interface gigabitethernet 1/1. <pre>FS# clear counters gigabitethernet 1/1</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.4 clear interface

	Use this command to reset the interface.	
	clear interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface ID
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command is only used on the switch port, member port of the L2 Aggregate port, routing port, and member port of the L3 aggregate port. This command is equal to the shutdown and no shutdown commands.	
Configuration Examples	The following example resets the interface gigabitethernet 1/1. <pre>FS# clear interface gigabitethernet 1/1</pre>	
Related Commands	Command	Description
	shutdown	Disables the interface.
Platform Description	N/A	

1.5 description

	Use this command to configure the alias of interface. Use the no form of this command to restore the default setting.	
	description <i>string</i>	
	no description	
Parameter Description	Parameter	Description
	<i>string</i>	Interface alias
Defaults	No alias is configured by default.	
Command Mode	Interface configuration mode.	
Usage Guide	Use show interfaces to display the interface information, including the alias.	

Configuration	The following example configures the alias of interface.	
Examples	<pre>FS(config)# interface gigabitethernet 1/1 FS(config-if)# description GBIC-1</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.6 duplex

	Use this command to specify the duplex mode for the interface. Use the no form of this command to restore the default setting.	
	duplex { auto full half }	
	no duplex	
Parameter Description	Parameter	Description
	auto	Self-adaptive full duplex and half duplex
	full	Full duplex
	half	Half duplex
Defaults	The default is auto ,	
Command Mode	Interface configuration mode.	
Usage Guide	The duplex mode is associated with the interface type. Use show interfaces to display the duplex mode of the interface	
Configuration Examples	The following example specifies the duplex mode for the interface. <pre>FS(config-if)# duplex full</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.7 errdisable recovery

	Use this command to recover the interface in violation.	
	errdisable recovery [<i>interval time</i>]	
Parameter Description	Parameter	Description
	<i>time</i>	Time for the command to take effect. The range is from 30 to 86,400 seconds.
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	Use the command to recover the port that triggers violation after being configured with the violation shutdown command.	
Configuration Examples	The following example recovers the violation interface gigabitethernet 1/1. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if)# errdisable recovery</pre>	
Related Commands	Command	Description
	switchport port-security violation shutdown	Configures the port security violation to shutdown.
Platform Description	N/A.	

1.8 fec mode

	Use this command to enable or disable the FEC function.	
	fec mode { <i>rs</i> <i>base-r</i> <i>none</i> <i>auto</i> }	
	Use the no form of this command to restore the default value.	
	no fec mode	
Parameter Description	Parameter	Description
	rs	Indicates the RS mode for enabling the FEC function.
	base-r	Indicates the base-r mode for enabling the FEC function.
	none	Disables the FEC function.
	auto	Indicates FEC function self-adaption, that is, the system determines whether to enable the FEC function based on the optical module and rate.

Defaults	The default configuration depends on the product model.
Command Mode	Interface configuration mode
Default Level	14
Usage Guide	When one end runs FEC function, the other end should enable it, too. On the premise of not affecting the negotiation status of the two ends, we suggest you NOT to: enable FEC function on the QSFP28-100G-LR4 optical module, on which FEC function is disabled by default. disable FEC function on QSFP28 modules (except QSFP28-100G-LR4), on which FEC function is enabled by default.
Configuration Examples	The following example forcibly enables the FEC function on Interface HundredGigabitEthernet 1/1. <pre>FS(config)# interface HundredGigabitEthernet 1/1 FS(config-if- HundredGigabitEthernet 1/1)# fec mode rs</pre> The following example forcibly enables the FEC function on Interface TFGigabitEthernet 2/1. <pre>FS(config)# interface TFGigabitEthernet 2/1 FS(config-if- TFGigabitEthernet 2/1)# fec mode base-r</pre>

1.9 fiber antifake enable

	Use this command to enable or disable the optical module antifake detection. Use the no form of this command to restore the default setting.	
	fiber antifake {ignore enable}	
	no fiber antifake enable	
Parameter Description	Parameter	Description
	ignore	Disables the optical module antifake detection.
	enable	Enables the optical module antifake detection.
Defaults	By default, optical module antifake detection is disabled.	
Command Mode	Global configuration mode	
Usage Guide	If the optical module antifake detection is enabled by default, when a non-original optical module is inserted, alarm logs are printed.	
Configuration Examples	The following example enables the optical module antifake detection. <pre>FS(config)# fiber antifake enable</pre>	
Related	Command	Description

Commands		
	N/A	N/A
Platform Description	N/A	

1.10 flowcontrol

	Use this command to enable or disable the flow control. Use the no form of this command to restore the default setting.	
	flowcontrol { auto off on }	
	no flowcontrol	
Parameter Description	Parameter	Description
	auto	Self-negotiates the flow control.
	off	Disables the flow control.
	on	Enables the flow control.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	Use the show interfaces command to display the flow control configuration.	
Configuration Examples	The following example enables flow control on fastEthernet port 1/1. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if)# flowcontrol on</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.11 interface

	Use this command to enter the interface configuration mode.	
	interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description

	<i>interface-type</i>	The interface type.
	<i>interface-number</i>	The interface ID.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enter interface configuration mode. The user can modify the interface configuration next,	
Configuration Examples	The following example enters configuration mode on Aggregateport 1. <pre>FS(config)# interface Aggregateport 1 FS(config-if-Aggregateport 1)#</pre> The following example enters configuration mode on GigabitEthernet 1/2. <pre>FS(config)# interface GigabitEthernet 1/2 FS(config-if-GigabitEthernet 1/2)#</pre> The following example configuration mode on VLAN 1. <pre>FS(config)# interface vlan 1 FS(config-if-VLAN 1)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.12 interface range

	Use this command to enter interface configuration mode on multiple interfaces.	
	interface range { <i>port-range</i> macro <i>macro_name</i> }	
	Use this command to define the macro name of the interface range command.	
	define interface-range <i>macro_name</i>	
Parameter Description	Parameter	Description
	<i>port-range</i>	The interface type and ID range, entered in the form of <i>interface-type slot-number/interface-number</i> . The interface can be either an Ethernet physical interface or a loopback interface.
	macro <i>macro_name</i>	The macro name which represents the interface range.
Defaults	The interface range command is disabled by default.	

Command Mode	Global configuration mode	
Usage Guide	Use the <code>define interface-range</code> command to define a range of interfaces as the macro name and then use the interface range macro macro_name command to enter interface configuration mode on multiple interfaces.	
Configuration Examples	The following example enters interface configuration mode on multiple interfaces by setting the interface range. <pre>FS(config)# interface range gigabitEthernet 0/0, 0/2 FS(config-if-range)# bandwidth 100</pre> The following example enters interface configuration mode on multiple interfaces by defining the macro name. <pre>FS(config)# define interface-range route1 gigabitEthernet 0/0-2 FS(config)# interface range macro route1 FS(config-if-range)# bandwidth 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.13 load-interval

	Use this command to set the interval for calculating load on the interface. Use the no form of this command to restore the default setting.	
	load-interval seconds	
	no load-interval	
Parameter Description	Parameter	Description
	seconds	In the range from 5 to 600 in the unit of seconds.
Defaults	The default is 10.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to set the interval for calculating load on the interface. In general, the numbers of incoming and outgoing packets and bytes are calculated every 10 seconds. For example, if the parameter is set to 180 seconds, the following outcome is displayed when the show interface gigabitEthernet 0/1 command is run. <pre>3 minutes input rate 15 bits/sec, 0 packets/sec 3 minutes output rate 14 bits/sec, 0 packets/sec</pre>	
Configuration Examples	The following example sets the interval for calculating load on interface GigabitEthernet 0/1 to 180 seconds. <pre>FS(config)# interface gigabitEthernet 0/1</pre>	

	FS(config-if-GigabitEthernet 0/1)# load-interval 180	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.14 logging

	Use this command to print information on the interface.	
	logging [link-updown error-frame link-dither]	
Parameter Description	Parameter	Description
	link-updown	Prints the status change information.
	error-frame	Prints the error frame information.
	link-dither	Prints the oscillation information.
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example prints information on the interface.. <pre>FS(config)# logging link-updown FS(config)# logging error-frame FS(config)# logging link-dither</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.15 mtu

	Use this command to set the MTU supported on the interface.	
	mtu <i>num</i>	

Parameter Description	Parameter	Description
	<i>num</i>	64 to 9216 (or 65536, which varies by products)
Defaults	The default is 1500.	
Command Mode	Interface configuration mode.	
Usage Guide	This command is used to set the maximum transmission unit (MTU) supported on the interface.	
Configuration Examples	The following example sets the MTU supported on interface gigabitethernet 1/1 to 9000. <pre>FS(config)# interface GigabitEthernet 1/1 FS(config-if-GigabitEthernet)# mtu 9000</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.16 negotiation mode

	Use this command to enable or disable auto-negotiation mode. Use the no form of this command to restore the default setting.	
	negotiation mode { on off }	
	no negotiation mode	
Parameter Description	Parameter	Description
	on	Enables auto-negotiation.
	off	Disables auto-negotiation.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	In general, the auto-negotiation status is determined by interface speed, duplex, and auto-negotiation factor mode.	
Configuration Examples	The following example enables auto-negotiation mode on interface GigabitEthernet 1/1. <pre>FS(config)# interface GigabitEthernet 1/1</pre>	

	FS(config-if-GigabitEthernet 1/1)# negotiation mode on	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.17 physical-port dither protect

	Use this command to enable oscillation protection on the port.	
	physical-port dither protect	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After you configure the physical-port dither protect command, the port will be shut down when the oscillation occurs for certain times.  If oscillation occurs on the port for 6 times within 2 seconds, a syslog will be printed. If syslog is printed for 10 consecutive times, the port will be shut down, If oscillation occurs on the port for over 10 times within 10 seconds, a syslog will be printed but the port will not be shut down.	
Configuration Examples	The following example enables oscillation protection on the port. <pre>FS(config)# physical-port dither protect</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.18 port speed-mode

	Use this command to configure the work rate mode of a 25 Gbps port.	
	port speed-mode {25G 10G }	

Parameter Description	Parameter	Description
	25G	Indicates that a 25 Gbps port works in 25 Gbps rate mode.
	10G	Indicates that a 25 Gbps port works in 10 Gbps rate mode.
Defaults	A 25 Gbps port works in 25 Gbps rate mode by default.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	1. Only 25 Gbps ports support this configuration. The four consecutive 25 Gbps ports of the same slot need to be set to work in the same rate mode. 2. Only 25 Gbps ports that work in the same rate mode can be added to the same aggregation group. 3. The default interface command will not clear the port speed-mode configuration of 25 Gbps ports.	
Configuration Examples	The following example configures Interfaces TFGigabitEthernet 2/1 through TFGigabitEthernet 2/4 to work in 10 Gbps rate mode. <pre> FS(config)# interface TFGigabitEthernet 2/2 FS(config-if-TFGigabitEthernet 2/2)# port speed-mode 10G Warning: Ports Tf2/1 – Tf2/4 will be set speed mode 10G. Continue? [Y/N]:Y FS(config-if-TFGigabitEthernet 2/2)# end </pre>	

1.19 protected-ports route-deny

	Use this command to configure L3 routing between the protected ports.	
	protected-ports route-deny	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default..	
Command Mode	Global configuration mode.	
Usage Guide	The ports that are set as the protected ports can route on L3. Use this command to deny the L3 communication between protected ports. Use the show running-config command to display configuration.	
Configuration Examples	The following example configures L3 routing between the protected ports. <pre> FS(config)# protected-ports route-deny </pre>	

Related Commands	Command	Description
	show running-config	Displays the protected ports route-deny configuration.
Platform Description	N/A	

1.20 show interfaces

	Use this command to display the interface information and optical module information.	
	show interfaces [<i>interface-type interface-number</i>] [description [up down]] [switchport trunk]	
Parameter Description	Parameter	Description
	<i>interface-id</i> <i>interface-number</i>	Interface (including Ethernet interface, aggregate port, SVI or loopback interface).
	description	The description of the interface, including the link status.
	switchport	Layer 2 interface information.
	trunk	Trunk port, applicable for physical port and aggregate port.
Defaults		
Command Mode	Privileged EXEC mode.	
Usage Guide	This command is used to show all basic information if no parameter is specified.	
Configuration Examples	The following example displays the interface information when the Gi0/1 is a Trunk port. <pre>SwitchA#show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is DOWN , line protocol is DOWN Hardware is Broadcom 5464 GigabitEthernet Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Carrier delay is 2 sec RXload is 1 ,Txload is 1 Queueing strategy: FIFO Output queue 0/0, 0 drops; Input queue 0/75, 0 drops Switchport attributes: interface's description:"" medium-type is copper</pre>	

```

lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
Priority is 0
admin duplex mode is AUTO, oper duplex is Unknown
admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin status is OFF,flow receive control oper status is
Unknown,flow send control oper status is Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control is OFF
Port-type: trunk
Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets

```

The following example displays the interface information when the Gi0/1 is an Access port.

```

SwitchA#show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Carrier delay is 2 sec
RXload is 1 ,Txload is 1
Queueing strategy: FIFO
Output queue 0/0, 0 drops;
Input queue 0/75, 0 drops
Switchport attributes:
interface's description:""
medium-type is copper
lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
Priority is 0
admin duplex mode is AUTO, oper duplex is Unknown
admin speed is AUTO, oper speed is Unknown
flow receive control admin status is OFF,flow send control admin status is OFF,flow receive control oper
status is Unknown,flow send control oper status is Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control is OFF
Port-type: access
Vlan id : 2

```

```

5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
        0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets

```

The following example displays the layer-2 interface information when the Gi0/1 is a Hybrid port.

```
SwitchA#show interfaces gigabitEthernet 0/1
```

```
Index(dec):1 (hex):1
```

```
GigabitEthernet 0/1 is DOWN , line protocol is DOWN
```

```
Hardware is Broadcom 5464 GigabitEthernet
```

```
Interface address is: no ip address
```

```
  MTU 1500 bytes, BW 1000000 Kbit
```

```
  Encapsulation protocol is Bridge, loopback not set
```

```
  Keepalive interval is 10 sec , set
```

```
  Carrier delay is 2 sec
```

```
  RXload is 1 ,Txload is 1
```

```
  Queueing strategy: FIFO
```

```
    Output queue 0/0, 0 drops;
```

```
    Input queue 0/75, 0 drops
```

```
Switchport attributes:
```

```
  interface's description:""
```

```
  medium-type is copper
```

```
  lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
```

```
  Priority is 0
```

```
  admin duplex mode is AUTO, oper duplex is Unknown
```

```
  admin speed is AUTO, oper speed is Unknown
```

```
  flow receive control admin status is OFF,flow send control admin status is OFF,flow receive control oper
status is Unknown,flow send control oper status is Unknown
```

```
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm Control is OFF
```

```
Port-type: hybrid
```

```
Tagged vlan id:2
```

```
Untagged vlan id:none
```

```
  5 minutes input rate 0 bits/sec, 0 packets/sec
```

```
  5 minutes output rate 0 bits/sec, 0 packets/sec
```

```
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
```

```
      Received 0 broadcasts, 0 runts, 0 giants
```

```
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
          0 packets output, 0 bytes, 0 underruns , 0 dropped
```

```
0 output errors, 0 collisions, 0 interface resets
```

The following example displays the layer-2 information of the Gi0/1.

	<pre>FS# show interfacesgigabitEthernet 0/1 switchport Interface Switchport ModeAccess Native Protected VLAN lists ----- GigabitEthernet 0/1 enabled Access 11 Disabled ALL</pre>	
Related Commands	Command	Description
	duplex	Duplex
	flowcontrol	Flow control status.
	interface gigabitEthernet	Selects the interface and enter the interface configuration mode.
	interface aggregateport	Creates or accesses the aggregate port, and enters the interface configuration mode.
	interface vlan	Creates or accesses the switch virtual interface (SVI), and enters the interface configuration mode.
	shutdown	Disables the interface.
	speed	Configures the speed on the port.
	switchport priority	Configures the default 802.1q interface priority.
	switchport protected	Configures the interface as a protected port.
Platform Description	N/A	

1.21 show interfaces counters

	Use this command to display the received and transmitted packet statistics.	
	show interfaces [<i>interface-type interface-number</i>] counters [increment drops errors rate summary] [<i>up</i> <i>down</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) The interface type and ID.
	increment	Displays the packet statistics increased during the last sample interval.
	drops	Displays dropped packet statistics.
	errors	Displays error packet statistics.
	rate	Displays packet receiving and transmitting rate.
	summary	Displays packet statistics summary.
	<i>up</i>	(Optional) Displays the port up statistics.
	<i>down</i>	(Optional) Displays the port down statistics.
Defaults	N/A	
Command Mode	Any CLI mode	

Usage Guide	If you do not specify an interface, the packet statistics on all interfaces are displayed.
Configuration	The following example displays packet statistics on interface GigabitEthernet 0/1.
Examples	<pre> FS#show interfaces GigabitEthernet 0/1 counters Interface : GigabitEthernet 0/1 5 minute input rate : 9144 bits/sec, 9 packets/sec 5 minute output rate : 1280 bits/sec, 1 packets/sec Rxload : 1% InOctets : 17310045 InPkts : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%) InUcastPkts : 100 InMulticastPkts : 100 InBroadcastPkts : 800 Txload : 1% OutOctets : 1282535 OutPkts : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%) OutUcastPkts : 100 OutMulticastPkts : 100 OutBroadcastPkts : 800 Undersize packets : 0 Oversize packets : 0 collisions : 0 Fragments : 0 Jabbers : 0 CRC alignment errors : 0 AlignmentErrors : 0 FCSErrors : 0 dropped packet events (due to lack of resources): 0 packets received of length (in octets): 64-127: 46264 128-255: 47427 256-511: 3478 512-1023: 658 1024-1518: 125 Packet increment in last sampling interval(5 seconds): InOctets : 10000 InPkts : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%) InUcastPkts : 100 InMulticastPkts : 100 InBroadcastPkts : 800 OutOctets : 10000 OutPkts : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%) </pre>

```
OutUcastPkts      : 100
OutMulticastPkts  : 100
```

i Rxload refers to the receive bandwidth usage and Txload refers to the Tx bandwidth usage. InPkts is the total number of receive unicast, multicast and broadcast packets. OutPkts is the total number of transmit unicast, multicast and broadcast packets.

Packet increment in last sampling interval (5 seconds) represents the packet statistics increased during the last sample interval (5 seconds).

The following example displays the packet statistics on interface GigabitEthernet 0/1 increased during the last sample interval.

```
FS#show interfaces GigabitEthernet 0/1 counters increment
```

```
Interface : GigabitEthernet 0/1
```

```
Packet increment in last sampling interval(5 seconds):
```

```
InOctets          : 10000
InPkts            : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts       : 100
InMulticastPkts   : 100
InBroadcastPkts   : 800
OutOctets          : 10000
OutPkts           : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts      : 100
OutMulticastPkts  : 100
```

The following example displays error packet statistics on interface GigabitEthernet 0/1.

```
FS#show interfaces GigabitEthernet 0/1 counters increment
```

Interface	UnderSize	OverSize	Collisions	Fragments
Gi0/1	0	0	0	0
Interface	Jabbers	CRC-Align-Err	Align-Err	FCS-Err
Gi0/1	0	0	0	0

i UnderSize is the number of valid packets smaller than 64 bytes.

OverSize is the number of valid packets smaller than 1518 bytes.

Collisions is the number of colliding transmit packets.

Fragments is the number of packets with CRC error or frame alignment error which are smaller than 64 bytes.

Jabbers is the number of packets with CRC error or frame alignment error which are smaller than 1518 bytes.

CRC-Align-Err is the number of receive packets with CRC error.

Align_Err is the number of receive packets with frame alignment error.

FCS-Err is the number of receive packets with FCS error.

The following example displays packet receiving and transmitting rate on interface GigabitEthernet 0/1.

```
FS#show interface gigabitEthernet 0/1 counters rate
```

Interface	Sampling Time	Input Rate	Input Rate	Output Rate
Output Rate		(bits/sec)	(packets/sec)	(bits/sec)
(packets/sec)				

	----- Gi0/15 seconds23391231240 -----																																						
	i Sampling Time is the time when packets are sampled. Input rate is packet receiving rate and Output rate is packet transmitting rate. -----																																						
	The following example displays packet statistics summary on interface GigabitEthernet 0/1.																																						
	FS#show interface gigabitEthernet 0/1 counters summary <table><tr><th>Interface</th><th>InOctets</th><th>InUcastPkts</th><th>InMulticastPkts</th><th>InBroadcastPkts</th></tr><tr><td colspan="5">-----</td></tr><tr><td>Gi0/1</td><td>1475788005</td><td>1389</td><td>45880503</td><td>11886621</td></tr><tr><th>Interface</th><th>OutOctets</th><th>OutUcastPkts</th><th>OutMulticastPkts</th><th>OutBroadcastPkts</th></tr><tr><td colspan="5">-----</td></tr><tr><td>Gi0/1</td><td>6667915</td><td>6382</td><td>31629</td><td>13410</td></tr><tr><td colspan="5">-----</td></tr></table> -----				Interface	InOctets	InUcastPkts	InMulticastPkts	InBroadcastPkts	-----					Gi0/1	1475788005	1389	45880503	11886621	Interface	OutOctets	OutUcastPkts	OutMulticastPkts	OutBroadcastPkts	-----					Gi0/1	6667915	6382	31629	13410	-----				
	Interface	InOctets	InUcastPkts	InMulticastPkts	InBroadcastPkts																																		

Gi0/1	1475788005	1389	45880503	11886621																																			
Interface	OutOctets	OutUcastPkts	OutMulticastPkts	OutBroadcastPkts																																			

Gi0/1	6667915	6382	31629	13410																																			

i InOctets is the total number of packets received on the interface. InUcastPkts is the number of unicast packets received on the interface. InMulticastPkts is the number of multicast packets received on the interface. InBroadcastPkts is the number of broadcast packets received on the interface. OutOctets is the total number of packets transmitted on the interface. OutUcastPkts is the number of unicast packets transmitted on the interface. OutMulticastPkts is the number of multicast packets transmitted on the interface. OutBroadcastPkts is the number of broadcast packets transmitted on the interface. -----																																							
Related Commands	Command		Description																																				
	N/A		N/A																																				
Platform Description	N/A																																						

1.22 show interfaces link-state-change statistics

	Use this command to display the link state change statistics, including the time and count.	
	show interfaces [<i>interface-type interface-number</i>] link-state-change statistics	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	The interface type and ID.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If you do not specify an interface, the link state statistics of all interfaces are displayed.	

Configuration Examples	The following example displays the link state statistics of interface GigabitEthernet 0/1.	
	FS#show int link-state-change statistics	
	Interface	Link state Link state change times Last change time Link-dither begin Link-dither end
	-----	-----
	Te0/1	down 0 2018-05-05 11:07:45 none
	none	
	Interface	Description
	Link state change times	The count of link state change.
	Last change time	The time when the last link state change occurs.
	Link-dither begin	The time when the last frequent dithers begin. "None" indicates no dither happens. Frequent dithers refer to six dithers happening within 2s.
	Link-dither end	The time when the last frequent dithers end. "None" indicates no dither happens.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.23 show interfaces status

	Use this command to display interface status information.	
	show interfaces [interface-type interface-number] status	
Parameter Description	Parameter	Description
	interface-type interface-number	The interface type and ID.
	status	Displays interface status information, including speed and duplex.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If you do not specify an interface, the status information of all interfaces is displayed.	

Configuration Examples	The following example displays the status information of interface GigabitEthernet 0/1.					
	FS#show interfaces GigabitEthernet 0/1 status					
	Interface	Status	Vlan	Duplex	Speed	Type
	-----	-----	-----	-----		
	GigabitEthernet 0/1	up	1	Full	1000M	copper
Related Commands	Command		Description			
	N/A		N/A			
Platform Description	N/A					

1.24 show interfaces status err-disable

	Use this command to display the interface violation status.							
	show interfaces [interface-type interface-number] status err-disable							
Parameter Description	Parameter	Description						
	<i>interface-type interface-number</i>	(Optional) The interface type and ID.						
Defaults								
Command Mode	Any CLI mode							
Usage Guide	If you do not specify an interface, violation status of all interfaces is displayed.							
Configuration Examples	The following example displays the violation status of interface GigabitEthernet 0/1. <pre>FS#show interface gigabitEthernet 0/1 status err-disabled</pre> <table> <tr> <th>Interface</th><th>Status</th><th>Reason</th></tr> <tr> <td>GigabitEthernet 0/1</td><td>err-disabled</td><td>BPDU Guard</td></tr> </table>  The violation status is displayed as err-disabled.		Interface	Status	Reason	GigabitEthernet 0/1	err-disabled	BPDU Guard
Interface	Status	Reason						
GigabitEthernet 0/1	err-disabled	BPDU Guard						
Related Commands	Command	Description						
	N/A	N/A						
Platform Description	N/A							

1.25 show interfaces transceiver

	Use this command to display transceiver information of the interface.	
	show interfaces [<i>interface-type interface-number</i>] transceiver [alarm diagnosis]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	The interface type and ID.
	transceiver	Displays the transceiver information.
	alarm	Displays the alarm message of the transceiver. If there is no alarm message, it is displayed as None.
	diagnosis	Displays the diagnostic parameters of the transceiver.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If you do not specify an interface, the transceiver information of all interfaces is displayed.	
Configuration Examples	The following example displays the transceiver information of interface GigabitEthernet 5/4. <pre>FS#show interfaces GigabitEthernet 5/4 transceiver Transceiver Type : 1000BASE-SX-SFP Connector Type : LC Wavelength(nm) : 850 Transfer Distance : 50/125 um OM2 fiber -- 550m 62.5/125 um OM1 fiber -- 270m Digital Diagnostic Monitoring : YES Vendor Serial Number : 101680093602489</pre> The following example displays the alarm message of the transceiver of interface GigabitEthernet 5/4. <pre>FS#show interfaces GigabitEthernet 5/4 transceiver alarm gigabitEthernet 5/4 transceiver current alarm information: RX loss of signal</pre> The following example displays the diagnostic parameters of the transceiver of interface GigabitEthernet 5/4. <pre>FS#show interfaces GigabitEthernet 5/4 transceiver diagnosis Current diagnostic parameters[AP:Average Power]: Temp(Celsius) Voltage(V) Bias(mA) RX power(dBm) TX power(dBm) 38(OK) 3.20(OK) 0.04(OK) -40.00(alarm)[AP] -40.00(alarm)</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.26 show interfaces usage

	Use this command to display bandwidth usage of the interface.																			
	show interfaces [<i>interface-type interface-number</i>] usage [<i>up</i> <i>down</i>]																			
Parameter Description	Parameter	Description																		
	<i>interface-type interface-number</i>	(Optional) The interface type and ID.																		
	<i>up</i>	(Optional) Displays the port up statistics.																		
	<i>down</i>	(Optional) Displays the port down statistics.																		
Defaults	N/A																			
Command Mode	Any CLI mode																			
Usage Guide	If you do not specify an interface, the bandwidth usage of all interfaces is displayed. Bandwidth refers to the actual link bandwidth rather than the <i>bandwidth</i> parameter configured on the interface.																			
Configuration Examples	The following example displays bandwidth usage of interface GigabitEthernet 0/1.																			
	<table><tr><th>Interface</th><th>Bandwidth</th><th>Average Usage</th><th>Output Usage</th><th>Input Usage</th></tr><tr><td colspan="5"> </td></tr><tr><td>GigabitEthernet 0/0</td><td>1000 Mbit</td><td>0.002822759%</td><td>0.001183280%</td><td>0.004462237%</td></tr></table>					Interface	Bandwidth	Average Usage	Output Usage	Input Usage						GigabitEthernet 0/0	1000 Mbit	0.002822759%	0.001183280%	0.004462237%
Interface	Bandwidth	Average Usage	Output Usage	Input Usage																
GigabitEthernet 0/0	1000 Mbit	0.002822759%	0.001183280%	0.004462237%																
	 Bandwidth refers to the interface link bandwidth, the maximum speed of link. Average Usage refers to the current usage.																			
Related Commands	Command		Description																	
	N/A		N/A																	
Platform Description	N/A																			

1.27 shutdown

	Use this command to disable an interface. Use the no form of this command to enable a disabled port.	
	shutdown	
	no shutdown	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the administrative status of an interface is Up.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to stop the forwarding on the interface (Gigabit Ethernet interface, Aggregate port or SVI). You can enable the port with the no shutdown command. If you shut down the interface, the configuration of the interface exists, but does not take effect. You can view the interface status by using the show interfaces command.  If you use the script to run no shutdown frequently and rapidly, the system may prompt the interface status reversal. 	
Configuration Examples	The following example disables an interface. <pre>FS(config)# interface aggregateport 1 FS(config-if)# shutdown</pre> The following example enables an interface. <pre>FS(config)# interface aggregateport 1 FS(config-if)# no shutdown</pre>	
Related Commands	Command	Description
	clear interface	Resets the hardware.
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.28 show split summary

	Use this command to display split information. show split summary																																		
Parameter Description	Parameter	Description																																	
	N/A	N/A																																	
Command Mode	All CLI user modes																																		
Default Level	14																																		
Usage Guide	This command displays split information of all splittable ports.																																		
Configuration Examples	The following example displays the split information about Interface GigabitEthernet 0/1. <pre>FS#show split summary</pre> <table border="1"> <thead> <tr> <th>Port</th><th>SpliteStatus</th><th>SplitPorts</th></tr> </thead> <tbody> <tr><td>Hu1/1</td><td>merged</td><td>Hu1/1:1 Hu1/1:2 Hu1/1:3 Hu1/1:4</td></tr> <tr><td>Hu1/2</td><td>merged</td><td>Hu1/2:1 Hu1/2:2 Hu1/2:3 Hu1/2:4</td></tr> <tr><td>Hu1/3</td><td>merged</td><td>Hu1/3:1 Hu1/3:2 Hu1/3:3 Hu1/3:4</td></tr> <tr><td>Hu1/4</td><td>merged</td><td>Hu1/4:1 Hu1/4:2 Hu1/4:3 Hu1/4:4</td></tr> <tr><td>Hu1/5</td><td>merged</td><td>Hu1/5:1 Hu1/5:2 Hu1/5:3 Hu1/5:4</td></tr> <tr><td>Hu1/6</td><td>merged</td><td>Hu1/6:1 Hu1/6:2 Hu1/6:3 Hu1/6:4</td></tr> <tr><td>Hu1/7</td><td>merged</td><td>Hu1/7:1 Hu1/7:2 Hu1/7:3 Hu1/7:4</td></tr> <tr><td>Hu1/8</td><td>merged</td><td>Hu1/8:1 Hu1/8:2 Hu1/8:3 Hu1/8:4</td></tr> <tr><td>Hu3/25</td><td>merged</td><td>Hu3/25:1 Hu3/25:2 Hu3/25:3 Hu3/25:4</td></tr> <tr><td>Hu3/26</td><td>merged</td><td>Hu3/26:1 Hu3/26:2 Hu3/26:3 Hu3/26:4</td></tr> </tbody> </table> Note: Port indicates the splittable master port, SpliteStatus indicates the current split status, and SplitPorts indicates member ports of the splittable port after splitting.		Port	SpliteStatus	SplitPorts	Hu1/1	merged	Hu1/1:1 Hu1/1:2 Hu1/1:3 Hu1/1:4	Hu1/2	merged	Hu1/2:1 Hu1/2:2 Hu1/2:3 Hu1/2:4	Hu1/3	merged	Hu1/3:1 Hu1/3:2 Hu1/3:3 Hu1/3:4	Hu1/4	merged	Hu1/4:1 Hu1/4:2 Hu1/4:3 Hu1/4:4	Hu1/5	merged	Hu1/5:1 Hu1/5:2 Hu1/5:3 Hu1/5:4	Hu1/6	merged	Hu1/6:1 Hu1/6:2 Hu1/6:3 Hu1/6:4	Hu1/7	merged	Hu1/7:1 Hu1/7:2 Hu1/7:3 Hu1/7:4	Hu1/8	merged	Hu1/8:1 Hu1/8:2 Hu1/8:3 Hu1/8:4	Hu3/25	merged	Hu3/25:1 Hu3/25:2 Hu3/25:3 Hu3/25:4	Hu3/26	merged	Hu3/26:1 Hu3/26:2 Hu3/26:3 Hu3/26:4
Port	SpliteStatus	SplitPorts																																	
Hu1/1	merged	Hu1/1:1 Hu1/1:2 Hu1/1:3 Hu1/1:4																																	
Hu1/2	merged	Hu1/2:1 Hu1/2:2 Hu1/2:3 Hu1/2:4																																	
Hu1/3	merged	Hu1/3:1 Hu1/3:2 Hu1/3:3 Hu1/3:4																																	
Hu1/4	merged	Hu1/4:1 Hu1/4:2 Hu1/4:3 Hu1/4:4																																	
Hu1/5	merged	Hu1/5:1 Hu1/5:2 Hu1/5:3 Hu1/5:4																																	
Hu1/6	merged	Hu1/6:1 Hu1/6:2 Hu1/6:3 Hu1/6:4																																	
Hu1/7	merged	Hu1/7:1 Hu1/7:2 Hu1/7:3 Hu1/7:4																																	
Hu1/8	merged	Hu1/8:1 Hu1/8:2 Hu1/8:3 Hu1/8:4																																	
Hu3/25	merged	Hu3/25:1 Hu3/25:2 Hu3/25:3 Hu3/25:4																																	
Hu3/26	merged	Hu3/26:1 Hu3/26:2 Hu3/26:3 Hu3/26:4																																	

1.29 snmp trap link-status

	Use this command to send LinkTrap on a port. Use the no form of this command to disable this function.	
	snmp trap link-status	
	no snmp trap link-status	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default	

Command Mode	Interface configuration mode.	
Usage Guide	For an interface (for instance, Ethernet interface, AP interface, and SVI interface), this command sets whether to send LinkTrap on the interface. If the function is enabled, the SNMP sends the LinkTrap when the link status of the interface changes.	
Configuration Examples	The following example disables the interface from sending LinkTrap on the interface. <pre>FS(config)# interface gigabitEthernet 1/1 FS(config-if)# no snmp trap link-status</pre> The following example enables the interface to forward Link trap. <pre>FS(config)# interface gigabitEthernet 1/1 FS(config-if)# snmp trap link-status</pre>	
Related Commands	Command	Description
	snmp trap link-status	Enables the interface to send LinkTrap on the interface.
	no snmp trap link-status	Disables the interface from sending LinkTrap on the interface.
Platform Description	N/A	

1.30 snmp-server if-index persist

	Use this command to set the interface index persistence. The interface index remains the same after the device is restarted.	
	snmp-server if-index persist	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After this command is configured, all interface indexes are saved in the configuration file. After the device is restarted, interface indexes remain the same as before.	
Configuration	The following example enables the interface index persistence.	

Examples	FS(config)# snmp-server if-index persist	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.31 speed

	Use this command to configure the speed on the port. speed [1000 10G 40G auto]	
Parameter Description	Parameter	Description
	1000	The transmission rate of the interface is 1000Mbps.
	10G	The transmission rate of the interface is 10Gbps.
	40G	The transmission rate of the interface is 40Gbps.
	auto	Self-adaptive
Defaults	The default is auto .	
Command Mode	Interface configuration mode.	
Usage Guide	If an interface is the member of an aggregate port, the rate of the interface depends on the rate of the aggregate port. You can set the rate of the interface, but it does not take effect until the interface exits the aggregate port. Use show interfaces to display configuration. The rate varies by interface types. For example, you cannot set the rate of a SFP interface to 10M.	
Configuration Examples	N/A	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.32 split interface

	Use this command to split a 40G interface into four 10G interfaces. Use the no form of this command to restore

	the default setting.	
	split interface FortyGigabitEthernet <i>interface-number</i>	
	no split interface FortyGigabitEthernet <i>interface-number</i>	
Parameter Description	Parameter	Description
	<i>interface-number</i>	Specifies the interface number.
Defaults	By default, the interface is in the combination mode.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example splits the 40G interface 0/65 into four 10G interfaces. FS(config-if)# split interface forty-giga 0/65	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.33 switchport

	Use this command to configure a Layer 3 interface. Use the no form of this command to restore the default setting.	
	switchport	
	no switchport	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	All the interfaces are in Layer 2 mode by default.	
Command Mode	Interface configuration mode.	
Usage Guide	This command is valid only for physical interfaces. The switchport command is used to disable the interface and re-enable it. In this status, the device will send the information to indicate the connect status. If the interface is	

	changed to Layer 3 mode from Layer 2, all the attributes in Layer 2 mode will be cleared.	
Configuration Examples	The following example configures a Layer 3 interface. FS(config-if)# switchport	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.34 switchport access

	Use this command to configure an interface as a statics access port and add it to a VLAN. Use the no form of this command to restore the default setting.	
	switchport access vlan <i>vlan-id</i>	
	no switchport access vlan	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN ID at which the port to be added.
Defaults	By default, the switch port is an access port and the VLAN is VLAN 1.	
Command Mode	Interface configuration mode.	
Usage Guide	Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the interface to the VLAN. If the port is a trunk port, the operation does not take effect.	
Configuration Examples	The following example configures interface gigabitethernet 1/1 as a statistic access port and adds it to VLAN 2. FS(config)# interface gigabitethernet 1/1 FS(config-if)# switchport access vlan 2	
Related Commands	Command	Description
	switchport mode	Configures the interface as Layer 2 mode (switch port mode).
	switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunkport.
Platform Description	N/A	

1.35 switchport mode

	Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port or an 802.1Q tunnel. Use the no form of this command to restore the default setting.	
	switchport mode { access trunk }	
	no switchport mode	
Parameter Description	Parameter	Description
	access	Configures the switch port as an access port.
	trunk	Configures the switch port as a trunk port.
Defaults	The default is access .	
Command Mode	Interface configuration mode.	
Usage Guide	If a switch port mode is access port, it can be the member port of only one VLAN. Use switchport access vlan to specify the member of the VLAN. A trunk port can be the member port of various VLANs defined by the allowed-VLAN list. The allowed VLAN list of the interface determines the VLANs to which the interface may belong. The trunk port is the member of all the VLANs in the allowed VLAN list. Use switchport trunk to define the allowed-VLANs list.	
Configuration Examples	The following example specifies a L2 interface (switch port) mode. <pre>FS(config-if)# switchport mode trunk</pre>	
Related Commands	Command	Description
	switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
	switchport trunk	Configures a native VLAN and the allowed-VLAN list for the trunk port.
Platform Description	N/A	

1.36 switchport protected

	Use this command to configure the interface as the protected port.	
	switchport protected	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	The ports that are set as the protected ports cannot switch on L2, but can route on L3. A protected port can communicate with an unprotected port. Use the show interfaces command to display configuration.	
Configuration Examples	The following example configures interface gigabitethernet 1/1 as a protected port. FS(config)#interface gigabitethernet 1/1 FS(config-if)# switchport protected	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
Platform Description	N/A	

1.37 switchport trunk

	Use this command to specify a native VLAN and the allowed-VLAN list for the trunk port. Use the no form of this command to restore the default setting.	
	switchport trunk { allowed vlan { all [add remove except] vlan-list } native vlan vlan-id }	
	no switchport trunk { allowed vlan native vlan }	
Parameter Description	Parameter	Description
	allowed vlan vlan-list	Configures the list of VLANs allowed on the trunk port. <i>vlan-list</i> can be a VLAN or a range of VLANs starting with the smaller VLAN ID and ending with the larger VLAN ID and being separated by hyphen, for example, 10 to 20. The segments can be separated with a comma (,), for example, 1 to 10, 20 to 25, 30, 33. all means that the allowed VLAN list contains all the supported VLANs; add means to add the specified VLAN list to the allowed VLAN list; remove means to remove the specified VLAN list from the allowed VLAN list; except means to add all the VLANs other than those in the specified VLAN list to the allowed VLAN list;
	native vlan vlan-id	Configures the native VLAN.
Defaults	The allowed VLAN list is all, the Native VLAN is VLAN1.	

Command Mode	Interface configuration mode.	
Usage Guide	Native VLAN: A trunk port belongs to one native VLAN. A native VLAN means that the untagged packets received/sent on the trunk port belong to the VLAN. Obviously, the default VLAN ID of the interface (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. In addition, when frames belonging to the native VLAN are sent over the trunk port, they are untagged. Allowed-VLAN List: By default, a trunk port sends traffic to and received traffic from all VLANs (ID 1 to 4094). However, you can prevent the traffic from passing over the trunk by configuring allowed VLAN lists on a trunk. Use show interfaces switchport to display configuration.	
Configuration Examples	The following example removes port 1/15 from VLAN 2. <pre>FS(config)# interface fastethernet 1/15 FS(config-if)# switchport trunk allowed vlan remove 2 FS(config-if)# end FS# show interfaces fastethernet1/15 switchport Switchport is enabled Mode is trunk port Access vlan is 1,Native vlan is 1 Protected is disabled Vlan lists is 1,3-4094</pre>	
Related Commands	Command	Description
	show interfaces	Displays the interface information.
	switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
Platform Description	N/A	

2 MAC Address Commands

2.1 clear mac-address-table dynamic

	Use this command to clear the dynamic MAC address.	
	clear mac-address-table dynamic [address <i>mac-addr</i> [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]] { [interface <i>interface-id</i>] [vlan <i>vlan-id</i>] }	
Parameter Description	Parameter	Description
	dynamic	Clears all the dynamic MAC addresses.
	address <i>mac-addr</i>	Clears the specified dynamic MAC address.
	interface <i>interface-id</i>	Clears all the dynamic MAC addresses of the specified interface.
	vlan <i>vlan-id</i>	Clears all the dynamic MAC addresses of the specified VLAN, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	Use the show mac-address-table dynamic command to display all the dynamic MAC addresses.	
Configuration Examples	The following command clears all the dynamic MAC addresses. FS# clear mac-address-table dynamic	
Related Commands	Command	Description
	show mac-address-table dynamic	Displays dynamic MAC address.
Platform Description	N/A	

2.2 mac-address-learning

	Use this command to enable the port address learning. Use the no or default form of this command to restore the default setting.	
	mac-address-learning	
	no mac-address-learning	
	default mac-address-learning	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The address learning function is enabled.	

Command Mode	Interface configuration mode.	
Usage Guide	MAC address learning cannot be disabled on the port where the security function is enabled. The security function cannot be configured on the port where address learning is disabled.	
Configuration Examples	The following example disables the port address learning function. <pre>FS(config-if)# no mac-address-learning</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.3 mac-address-learning (global)

	Use this command to enable MAC address learning globally. Use the no or default form of this command to restore the default setting.	
	mac-address-learning enable	
	Use this command to disable MAC address learning globally.	
	mac-address-learning disable	
	Use this command to restore MAC address learning globally.	
	default mac-address-learning	
Parameter Description	Parameter	Description
	enable	Enables MAC address learning globally.
	disable	Disables MAC address learning globally.
Defaults	The mac-address-learning enable command is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	When this function is enabled, the MAC address is learned in global configuration mode the same as learned in interface configuration mode.	
Configuration Examples	The following example disables MAC address learning globally. <pre>FS(config)# mac-address-learning disable</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

2.4 mac-address-table aging-time

	Use this command to specify the aging time of the dynamic MAC address. Use the no or default form of the command to restore the default setting.	
	mac-address-table aging-time <i>seconds</i>	
	no mac-address-table aging-time default mac-address-table aging-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	Aging time of the dynamic MAC address (in seconds). The time range depends on the switch.
Defaults	The default is 300.	
Command Mode	Global configuration mode.	
Usage Guide	Use show mac-address-table aging-time to display configuration.	
Configuration Examples	The following example sets the aging time of the dynamic MAC address to 500 seconds. FS(config)# mac-address-table aging-time 500	
Related Commands	Command	Description
	show mac-address-table aging-time	Displays the aging time of the dynamic MAC address.
	show mac-address-table dynamic	Displays dynamic MAC address.
Platform	N/A	
Description		

2.5 mac-address-table filtering

	Use this command to configure the filtering MAC address. Use the no or default form of the command to restore the default setting.	
	mac-address-table filtering <i>mac-address</i> vlan <i>vlan-id</i>	
	no mac-address-table filtering <i>mac-address</i> vlan <i>vlan-id</i> default mac-address-table filtering <i>mac-address</i> vlan <i>vlan-id</i>	
Parameter Description	Parameter	Description
	<i>mac-address</i>	Filtering Address
	<i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.

Defaults	No filtering address is configured by default.				
Command Mode	Global configuration mode.				
Usage Guide	The filtering MAC address shall not be a multicast address.				
Configuration Examples	The following example configures the filtering MAC address for VLAN 1. <pre>FS(config)#mac-address-table filtering 0000.0202.0303 vlan 3</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>clear mac-address-table filtering</td><td>Clears the filtering MAC address.</td></tr> </table>	Command	Description	clear mac-address-table filtering	Clears the filtering MAC address.
Command	Description				
clear mac-address-table filtering	Clears the filtering MAC address.				
Platform Description	N/A				

2.6 mac-address-table notification

	Use this command to enable the MAC address notification function. Use The no or default form of the command to restore the default setting.	
	mac-address-table notification [interval <i>value</i> history-size <i>value</i>]	
	no mac-address-table notification [interval history-size] default mac-address-table notification [interval history-size]	
Parameter Description	Parameter	Description
	interval <i>value</i>	Sets the interval of sending the MAC address trap message, 1 second by default.
	history-size <i>value</i>	Sets the maximum number of the entries in the MAC address notification table, 50 entries by default.
Defaults	By default, the interval is 1 and the maximum number of the entries in the MAC address notification table is 50.	
Command Mode	Global configuration mode.	
Usage Guide	The MAC address notification function is specific for only dynamic MAC address and secure MAC address. No MAC address trap message is generated for static MAC addresses. In the global configuration mode, you can use the snmp-server enable traps mac-notification command to enable or disable the switch to send the MAC address trap message.	
Configuration Examples	The following example enables the MAC address notification function. FS(config)# mac-address-table notification FS(config)# mac-address-table notification interval 40	

	FS(config)# mac-address-table notification history-size 100	
Related Commands	Command	Description
	snmp-server enable traps	Sets the method of handling the MAC address trap message..
	show mac-address-table notification	Displays the MAC address notification configuration and the MAC address trap notification table.
	snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.
Platform Description	N/A	

2.7 mac-address-table static

	Use this command to configure a static MAC address. Use the no or default form of the command to restore the default setting.	
	mac-address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i>	
	no mac-address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i>	
	default mac-address-table static <i>mac-addr</i> vlan <i>vlan-id</i> interface <i>interface-id</i>	
Parameter Description	Parameter	Description
	<i>mac-addr</i>	Destination MAC address of the specified entry
	<i>vlan-id</i>	VLAN ID of the specified entry, in the range from 1 to 4094.
	<i>interface-id</i>	Interface (physical interface or aggregate port) that packets are forwarded to
Defaults	No static MAC address is configured by default.	
Command Mode	Global configuration mode.	
Usage Guide	A static MAC address has the same function as the dynamic MAC address that the switch learns. Compared with the dynamic MAC address, the static MAC address will not be aged out. It can only be configured and removed by manual. Even if the switch is reset, the static MAC address will not be lost. A static MAC address shall not be configured as a multicast address. Use show mac-address-table static to display the static MAC address.	
Configuration Examples	N/A	
Related Commands	Command	Description
	show mac-address-table static	Displays the static MAC address.
Platform Description	N/A	

2.8 max-dynamic-mac-count

	Use this command to set the maximum number of MAC address learned dynamically on the VLAN or interface. Use the no or default form of this command to restore the default setting.	
	max-dynamic-mac-count <i>num</i>	
	no max-dynamic-mac-count	
	default max-dynamic-mac-count	
Parameter Description	Parameter	Description
	<i>num</i>	Sets the maximum number of MAC addresses.
Defaults	The maximum number is not set by default.	
Command Mode	VLAN configuration mode / Interface configuration mode	
Usage Guide	This command is used to set the maximum number of MAC addresses learned dynamically on the VLAN or interface. If the number of MAC addresses dynamically learned on the VLAN or interface reaches the upper limit, MAC address learning is disabled on the VLAN or interface. If the number of MAC addresses reaches the upper limit when this command is configured, the surplus MAC addresses are not cleared. Instead, they remain and then age. MAC address learning is disabled on the VLAN or interface. Use the show mac-address-table max-dynamic-mac-count command to display the maximum number of MAC addresses learned dynamically on the VLAN or interface.	
Configuration Examples	The following example sets the maximum number of MAC addresses dynamically learned on VLAN 1. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#vlan 1 FS(config-vlan)#max-dynamic-mac-count 160</pre> The following example sets the maximum number of MAC addresses dynamically learned on interface GigabitEthernet 0/1. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 160</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.9 max-dynamic-mac-count exceed-action

	Use this command to set the action if the dynamic MAC address learned on the VLAN or interface exceeds the limit. Run the no form of this command to restore the default setting.	
	max-dynamic-mac-count exceed-action forward discard	
	no max-dynamic-mac-count exceed-action forward discard	
Parameter Description	Parameter	Description
	<i>forward</i>	Forwards the packets if the dynamic MAC address learned on the VLAN or interface exceeds the limit.
	<i>discard</i>	Discards the packets if the dynamic MAC address learned on the VLAN or interface exceeds the limit.
Command Mode	VLAN configuration mode / Interface configuration mode	
Usage Guide	This command is used to set the action if the dynamic MAC address learned on the VLAN or interface exceeds the limit. When the command default interface is run in global configuration mode, if there is any layer-2 sub-interface, the action when MAC address learned dynamically exceeds the limit cannot restore the default settings.	
Configuration Examples	The following example sets the maximum number of MAC addresses dynamically learned on VLAN 1. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#vlan 1 FS(config-vlan)#max-dynamic-mac-count 160 FS(config-vlan)#max-dynamic-mac-count exceed-action discard</pre> The following example sets the maximum number of MAC addresses dynamically learned on interface GigabitEthernet 0/1. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count 100 FS(config-if-GigabitEthernet 0/1)#max-dynamic-mac-count exceed-action discard</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.10 show mac-address-learning

	Use this command to display the MAC address learning.	
	show mac-address-learning	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the MAC address learning. <pre> FS# show mac-address-learning GigabitEthernet 0/0 learning ability: disable GigabitEthernet 0/1 learning ability: enable GigabitEthernet 0/2 learning ability: enable GigabitEthernet 0/3 learning ability: enable </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.11 show mac-address-table

	Use this command to display all types of MAC addresses (including dynamic address, static address and filter address).	
	show mac-address-table [address <i>mac-addr</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	address <i>mac-addr</i>	The MAC address.
	interface <i>interface-id</i>	The Interface ID.
	vlan <i>vlan-id</i>	The VLAN ID, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	All modes	

Usage Guide	N/A																																														
Configuration Examples	The following example displays the MAC address. FS# show mac-address-table address 00d0.f800.1001 <table><tr><td>Vlan</td><td>MAC Address</td><td>Type</td><td>Interface</td></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>1</td><td>00d0.f800.1001</td><td>STATIC</td><td>GigabitEthernet 1/1</td></tr></table> FS# show mac-address-table <table><tr><td>Vlan</td><td>MAC Address</td><td>Type</td><td>Interface</td></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>1</td><td>00d0.f800.1001</td><td>STATIC</td><td>GigabitEthernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1002</td><td>DYNAMIC</td><td>GigabitEthernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1003</td><td>OTHER</td><td>GigabitEthernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1004</td><td>FILTER</td><td></td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Vlan</td><td>The interface address.</td></tr><tr><td>MAC Address</td><td>The MAC address.</td></tr><tr><td>Type</td><td>The MAC address type.</td></tr><tr><td>Interface</td><td>The interface corresponding to the MAC address.</td></tr></table>	Vlan	MAC Address	Type	Interface	-----	-----	-----	-----	1	00d0.f800.1001	STATIC	GigabitEthernet 1/1	Vlan	MAC Address	Type	Interface	-----	-----	-----	-----	1	00d0.f800.1001	STATIC	GigabitEthernet 1/1	1	00d0.f800.1002	DYNAMIC	GigabitEthernet 1/1	1	00d0.f800.1003	OTHER	GigabitEthernet 1/1	1	00d0.f800.1004	FILTER		Field	Description	Vlan	The interface address.	MAC Address	The MAC address.	Type	The MAC address type.	Interface	The interface corresponding to the MAC address.
Vlan	MAC Address	Type	Interface																																												
-----	-----	-----	-----																																												
1	00d0.f800.1001	STATIC	GigabitEthernet 1/1																																												
Vlan	MAC Address	Type	Interface																																												
-----	-----	-----	-----																																												
1	00d0.f800.1001	STATIC	GigabitEthernet 1/1																																												
1	00d0.f800.1002	DYNAMIC	GigabitEthernet 1/1																																												
1	00d0.f800.1003	OTHER	GigabitEthernet 1/1																																												
1	00d0.f800.1004	FILTER																																													
Field	Description																																														
Vlan	The interface address.																																														
MAC Address	The MAC address.																																														
Type	The MAC address type.																																														
Interface	The interface corresponding to the MAC address.																																														
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A																																										
Command	Description																																														
N/A	N/A																																														
Platform Description	N/A																																														

2.12 show mac-address-table aging-time

	Use this command to display the aging time of the dynamic MAC address.	
	show mac-address-table aging-time	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	All modes	
Usage Guide	N/A	
Configuration Examples	The following example displays the aging time of the dynamic MAC address. FS# show mac-address-table aging-time Aging time : 300	

Related Commands	Command	Description
	mac-address-table aging-time	Sets the aging time of the dynamic MAC address.
Platform	N/A	
Description		

2.13 show mac-address-table count

	Use this command to display the number of address entries in the address table.	
	show mac-address-table count [interface <i>interface-id</i> vlan <i>vlan-id</i>]	
Parameter	Parameter	Description
Description	interface <i>interface-id</i>	Interface ID
	vlan <i>vlan-id</i>	VLAN ID, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	The show mac-address-table count command is used to display the number of entries based on the type of MAC address entry. The show mac-address-table count interface command is used to display the number of entries based on the interface associated with the MAC address entry. The show mac-address-table count vlan command is used to display the number of entries based on the VLAN of MAC address entries.	
Configuration Examples	The following example displays the number of MAC address entries. <pre>FS# show mac-address-table count Dynamic Address Count : 51 Static Address Count : 0 Filter Address Count : 0 Total Mac Addresses : 51 Total Mac Address Space Available: 8139</pre> The following example displays the number of MAC address in VLAN 1. <pre>FS# show mac-address-table count vlan 1 Dynamic Address Count : 7 Static Address Count : 0 Filter Address Count : 0 Total Mac Addresses : 7</pre> The following example displays the number of MAC addresses on interface g0/1. <pre>FS# show mac-address-table interface g0/1 Dynamic Address Count : 10</pre>	

	Static Address Count : 0 Filter Address Count : 0 Total Mac Addresses : 10	
Related Commands	Command	Description
	show mac-address-table static	Displays the static address.
	show mac-address-table filtering	Displays the filtering address.
	show mac-address-table dynamic	Displays the dynamic address.
	show mac-address-table address	Displays all the address information of the specified address.
	show mac-address-table interface	Displays all the address information of the specified interface.
	show mac-address-table vlan	Displays all the address information of the specified vlan.
Platform Description	N/A	

2.14 show mac-address-table dynamic

	Use this command to display the dynamic MAC address.	
	show mac-address-table dynamic [address <i>mac-add r</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	<i>mac-addr</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN of the entry, in the range from 1 to 4094.
	<i>interface-id</i>	Interface that the packet is forwarded to. It may be a physical port or an aggregate port
Defaults		
Command Mode	All modes	
Usage Guide	N/A	
Configuration Examples	The following example displays the dynamic MAC address.	
	FS# show mac-address-table dynamic <pre> Vlan MAC Address Type Interface ----- 1 0000.0000.0001 DYNAMIC gigabitethernet 1/1 1 0001.960c.a740 DYNAMIC gigabitethernet 1/1 1 0007.95c7.dff9 DYNAMIC gigabitethernet 1/1 1 0007.95cf.eee0 DYNAMIC gigabitethernet 1/1 1 0007.95cf.f41f DYNAMIC gigabitethernet 1/1 1 0009.b715.d400 DYNAMIC gigabitethernet 1/1 1 0050.bade.63c4 DYNAMIC gigabitethernet 1/1 </pre>	

Related Commands	Command	Description
	clear mac-address-table dynamic	Clears the dynamic MAC address.
Platform Description	N/A	

2.15 show mac-address-table filtering

	Use this command to display the filtering MAC address.	
	show mac-address-table filtering [ddr <i>mac-addr</i>] [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	<i>mac-addr</i>	Destination MAC address of the entry
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the filtering MAC address. <pre>FS# show mac-address-table filtering Vlan MAC Address Type Interface ----- 1 0000.2222.2222 FILTER Not available</pre>	
Related Commands	Command	Description
	mac-address-table filtering	Configures the filtering MAC address.
Platform Description	N/A	

2.16 show mac-address-table interface

	Use this command to display all the MAC addresses on the specified interface including static and dynamic MAC address	
	show mac-address-table interface [<i>interface-id</i>] [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Displays the MAC address information of the specified Interface (physical interface or aggregate port).
	<i>vlan-id</i>	VLAN ID of the entry, in the range from 1 to 4094..

Defaults	N/A																					
Command Mode	Privileged EXEC mode.																					
Usage Guide	N/A																					
Configuration Examples	The following example displays all the MAC addresses on interface gigabitethernet 1/1. <pre>FS# show mac-address-table interface gigabitethernet 1/1</pre> <table><thead><tr><th>Vlan</th><th>MAC Address</th><th>Type</th><th>Interface</th></tr></thead><tbody><tr><td>1</td><td>00d0.f800.1001</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1002</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1003</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1004</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr></tbody></table>		Vlan	MAC Address	Type	Interface	1	00d0.f800.1001	STATIC	gigabitethernet 1/1	1	00d0.f800.1002	STATIC	gigabitethernet 1/1	1	00d0.f800.1003	STATIC	gigabitethernet 1/1	1	00d0.f800.1004	STATIC	gigabitethernet 1/1
Vlan	MAC Address	Type	Interface																			
1	00d0.f800.1001	STATIC	gigabitethernet 1/1																			
1	00d0.f800.1002	STATIC	gigabitethernet 1/1																			
1	00d0.f800.1003	STATIC	gigabitethernet 1/1																			
1	00d0.f800.1004	STATIC	gigabitethernet 1/1																			
Related Commands	Command	Description																				
	show mac-address-table static	Displays the static MAC address.																				
	show mac-address-table filtering	Displays the filtering MAC address.																				
	show mac-address-table dynamic	Displays the dynamic MAC address.																				
	show mac-address-table address	Displays all types of MAC addresses.																				
	show mac-address-table vlan	Displays all types of MAC addresses of the specified VLAN.																				
	show mac-address-table count																					
	Displays the address counts in the MAC address table.																					
Platform Description	N/A																					

2.17 show mac-address-table max-dynamic-mac-count

	Use this command to display the maximum number of dynamic MAC addresses learned on the VLAN or interface.	
	show mac-address-table max-dynamic-mac-count { vlan [<i>vlan-id</i>] interface [<i>interface-id</i>] }	
Parameter Description	Parameter	Description
	vlan	Displays the dynamic MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC address learning.
	<i>vlan-id</i>	Displays the dynamic MAC address learned on the specified VLAN.
	interface	Displays the dynamic MAC address learned on all interfaces which are configured with the maximum number of dynamic MAC address learning.
	<i>interface-id</i>	Displays the dynamic MAC address learned on the specified interface.

Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the MAC address learned on all VLANs which are configured with the maximum number of dynamic MAC addresses.	
	<pre>FS#show mac-address-table max-dynamic-mac-count vlan</pre>	
	<pre>Vlan Limit MAC count Learning</pre>	
	<pre>-----</pre>	
	<pre>1 160 6 YES</pre>	
	The following example displays the MAC address learned dynamically on the specified VLAN.	
	<pre>FS#show mac-address-table max-dynamic-mac-count vlan 1</pre>	
	<pre>Vlan Limit MAC count Learning</pre>	
	<pre>-----</pre>	
	<pre>1 160 6 YES</pre>	
</		

Platform	N/A
Description	

2.18 show mac-address-table notification

	Use this command to display the MAC address notification configuration and the MAC address notification table.	
	show mac-address-table notification [interface [<i>interface-id</i>] history]	
Parameter	Parameter	Description
Description	interface	Displays the MAC address notification configuration on all interfaces.
	<i>interface-id</i>	Displays the MAC address notification configuration on a specific interface.
	history	Displays the MAC address notification history.
Defaults		
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the MAC address notification configuration and the MAC address notification table. <pre>FS# show mac-address-table notification MAC Notification Feature: Disabled Interval between Notification Traps: 1 secs Maximum Number of entries configured in History Table:1 Current History Table Length: 0</pre>	
Related Commands	Command	Description
	mac-address-table notification	Enables MAC address notification.
	snmp trap mac-notification	Enables the MAC address trap notification function on the specified interface.
Platform	N/A	
Description		

2.19 show mac-address-table static

	Use this command to display the static MAC address.	
	show mac-address-table static [addr <i>mac-addr</i>] [interface <i>interface-id</i>] [vlan <i>vlan-id</i>]	
Parameter	Parameter	Description
Description	<i>mac-addr</i>	Destination MAC address of the entry

	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.																				
	<i>interface-id</i>	Interface of the entry physical interface or aggregate port																				
Defaults	N/A																					
Command Mode	Privileged EXEC mode.																					
Usage Guide	N/A																					
Configuration Examples	The following example displays the static MAC addresses																					
	<pre>FS# show mac-address-table static</pre> <table><tr><th>Vlan</th><th>MAC Address</th><th>Type</th><th>Interface</th></tr><tr><td colspan="4">-----</td></tr><tr><td>1</td><td>00d0.f800.1001</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1002</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr><tr><td>1</td><td>00d0.f800.1003</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr></table>		Vlan	MAC Address	Type	Interface	-----				1	00d0.f800.1001	STATIC	gigabitethernet 1/1	1	00d0.f800.1002	STATIC	gigabitethernet 1/1	1	00d0.f800.1003	STATIC	gigabitethernet 1/1
Vlan	MAC Address	Type	Interface																			

1	00d0.f800.1001	STATIC	gigabitethernet 1/1																			
1	00d0.f800.1002	STATIC	gigabitethernet 1/1																			
1	00d0.f800.1003	STATIC	gigabitethernet 1/1																			
Related Commands	Command mac-address-table static	Description Configures the static MAC address.																				
Platform Description	N/A																					

2.20 show mac-address-table vlan

	Use this command to display all addresses of the specified VLAN.									
	show mac-address-table vlan [<i>vlan-id</i>]									
Parameter	Parameter	Description								
Description	<i>vlan-id</i>	VLAN ID of the entry, within the range from 1 to 4094.								
Defaults	N/A									
Command Mode	Privileged EXEC mode									
Usage Guide	N/A									
Configuration Examples	The following example displays all addresses of the specified VLAN. FS# show mac-address-table vlan 1 <table><tr><th>Vlan</th><th>MAC Address</th><th>Type</th><th>Interface</th></tr><tr><td>1</td><td>00d0.f800.1001</td><td>STATIC</td><td>gigabitethernet 1/1</td></tr></table>		Vlan	MAC Address	Type	Interface	1	00d0.f800.1001	STATIC	gigabitethernet 1/1
Vlan	MAC Address	Type	Interface							
1	00d0.f800.1001	STATIC	gigabitethernet 1/1							

	1	00d0.f800.1002	STATIC	gigabitethernet 1/1
	1	00d0.f800.1003	STATIC	gigabitethernet 1/1
Related Commands	Command			Description
	show mac-address-table static			Displays static addresses.
	show mac-address-table filtering			Displays filtered addresses.
	show mac-address-table dynamic			Displays dynamic addresses.
	show mac-address-table address			Displays all address information about the specified address.
	show mac-address-table interface			Displays all address information about the specified interface.
	show mac-address-table count			Displays the number of addresses in the address table.
Platform Description	N/A			

2.21 snmp trap mac-notification

	Use this command to enable the MAC address trap notification on the specified interface. Use The no or default form of the command to restore the default setting.	
	snmp trap mac-notification { added removed }	
	no snmp trap mac-notification { added removed } default snmp trap mac-notification { added removed }	
Parameter Description	Parameter	Description
	added	Notifies when a MAC address is added.
	removed	Notifies when a MAC address is removed
Defaults		
Command Mode	Interface configuration mode.	
Usage Guide	Use show mac-address-table notification interface to display configuration.	
Configuration Examples	The following example enables the MAC address trap notification on interface gigabitethernet 1/1. FS(config)# interface gigabitethernet 1/1 FS(config-if)# snmp trap mac-notification added	
Related Commands	Command	Description
	mac-address-table notification	Enables MAC address notification.
	show mac-address-table notification	Displays the MAC address notification configuration and the MAC address notification table.
Platform Description	N/A	

3 Aggregate Port Commands

3.1 aggregate bfd-detect

	Use this command to enable BFD on the AP port. Use the no form of this command to restore the default setting.	
	aggregate bfd-detect ipv4 <i>src_ip dst_ip</i>	
	no aggregate bfd-detect ipv4	
Parameter Description	Parameter	Description
	ipv4	Enables IPv4 BFD when the AP port is configured with an IPv4 address.
	<i>src_ip</i>	Specifies source IP address, namely, the IP address configured on the AP port.
	<i>dst_ip</i>	Specifies destination IP address, namely, the IP address configured on the peer AP port.
Defaults	This function is disabled by default.	
Command Mode	AP interface configuration mode	
Usage Guide	If you want to enable BFD on the AP port, you should see corresponding configuration guide for BFD parameter settings. Different products vary in support for IPv4 BFD on AP port. If an AP port supports IPv4 BFD, it is allowed to enable IPv4 BFD at the same time. If an AP port is enabled with BFD, its member ports in forwarding state create BFD session automatically.	
Configuration Examples	The following example enables BFD on the AP port. <pre>Switch(config)# interface aggregateport 3 Switch(config-if-Aggregateport 3)# ip address 1.0.0.1 Switch(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2 Switch(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.2 aggregateport capacity mode

	Use this command to configure the AP capacity mode. Use the no form of this command to restore the default setting, Use the no form of this command to restore the default setting,

	aggregateport capacity mode <i>capacity-mode</i>	
	no aggregateport capacity mode	
Parameter Description	Parameter	Description
	<i>capacity-mode</i>	Configures the capacity mode.
Defaults	The default <i>capacity-mode</i> varies with the device.	
Command Mode	Global configuration mode	
Usage Guide	The system provides several capacity modes for devices that support capacity mode configuration. To restore the default settings, run no aggregateport capacity mode in global configuration mode.	
Configuration Examples	The following example configures the the capacity mode.	
	<pre>FS# configure terminal FS(config)# aggregateport capacity mode 256*8</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.3 aggregateport hash-header

	Use this command to specify the balancing factor acquisition mode for specific tunnel packets, to optimize traffic balancing. Use the default form of this command to restore the default setting,	
	aggregateport hash-header {inner outer}	
	default aggregateport hash-header	
Parameter Description	Parameter	Description
	inner	Specifies the inner layer in the header of tunnel packets as the source for acquiring the balancing factor.
	outer	Specifies the outer layer in the header of tunnel packets as the source for acquiring the balancing factor.
Defaults	The default configuration varies with products.	
Command Mode	Global configuration mode	
Usage Guide	Optional. When performing load balancing, use this command to specify the balancing factor acquisition mode	

	for specific tunnel packets, to optimize traffic balancing. Use the default form of this command to restore the default acquisition mode. After configuration, if the show running command does not display the configuration, the configured mode is the same as the default value.  The supported configuration options and types of tunnel packets vary with products.	
Configuration Examples	The following example specifies the inner layer in the header of tunnel packets as the source for acquiring the balancing factor in global configuration mode. <pre>FS# configure terminal FS(config)# aggregateport hash-header inner</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.4 aggregateport load-balance

	Use this command to configure a global load-balance algorithm for aggregate ports or a load-balance algorithm for an aggregate port . Use the no form of this command to return the default setting.	
	aggregateport load-balance { dst-mac src-mac src-dst-mac dst-ip src-ip src-dst ip src-dst-ip-l4port enhanced profile <i>profile-name</i> }	
	no aggregateport load-balance	
Parameter Description	Parameter	Description
	dst-mac	Load balance based on the destination MAC addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination MAC addresses are sent to the same port, and those with different destination MAC addresses are sent to different ports.
	src-mac	Load balance based on the source MAC addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and those from the same addresses are distributed to the same port.
	src-dst-ip	Load balance based on the source IP address and destination IP address. Packets with different source and destination IP address pairs are forwarded through different ports. The packets with the same source and destination IP address pairs are forwarded through the same links. At layer 3, this load balancing style is recommended.
	dst-ip	Load balance based on the destination IP addresses of the incoming packets. For all the links of an aggregate port, the messages with the same destination IP addresses are sent to the same port, and those with different destination IP addresses are sent to different ports.
	src-ip	Load balance based on the source IP addresses of the incoming packets. For all the links of an aggregate port, the messages from different addresses are distributed to different ports, and

		those from the same addresses are distributed to the same port.				
	src-dst-mac	Load balance based on the source and destination MAC addresses. Packets with different source and destination MAC address pairs are forwarded through different ports. The packets with the same source and destination MAC address pairs are forwarded through the same port.				
	src-dst-ip-l4port (supported in global configuration mode)	Load balance based on the source IP address, destination IP address, L4 source port number and L4 destination port number.				
	enhanced profile	Load balance based on the packet type				
Defaults	The default load balance mode is src-dst-mac for the L2 AP port and src-dst-ip for the L3 AP port .					
Command Mode	Global configuration mode/Interface configuration mode					
Usage Guide	You can run aggregateport load-balance in interface configuration mode of an AP port on devices that support load balancing configuration on a specific AP port. The configuration in interface configuration mode prevails. To disable the load balancing algorithm, run no aggregateport load-balance in interface configuration mode of the AP port. After that, the load balancing algorithm configured in global configuration mode takes effect.					
Configuration Examples	The following example configures a load-balance algorithm globally based on the destination MAC address. FS(config)# aggregateport load-balance dst-mac					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show aggregateport load-balance</td><td>Displays aggregate port configuration.</td></tr></table>	Command	Description	show aggregateport load-balance	Displays aggregate port configuration.	
Command	Description					
show aggregateport load-balance	Displays aggregate port configuration.					
Platform Description	N/A					

3.5 aggregateport member linktrap

	Use this command to send LinkTrap to aggregate port members. Use the no form of this command to restore the default setting.	
	aggregateport member linktrap	
	no aggregateport member linktrap	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Global configuration mode	
Usage Guide	This function cannot be enabled by running the snmp trap link-status command in interface configuration mode.	
Configuration Examples	The following example enables the LinkTrap function on the aggregate port members. <pre>FS# configure terminal FS(config)# aggregateport member linktrap</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.6 aggregateport primary-port

	Use this command to configure the AP member port as a primary port. Use the no form of this command to restore the default setting.	
	aggregateport primary-port	
	no aggregateport primary-port	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The AP member port is not a primary port by default.	
Command Mode	Interface configuration mode	
Usage Guide	Only one primary port can be configured for an aggregate port.	
Configuration Examples	The following example configures GigabitEthernet 0/1 as a primary port. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# port-group 1 mode active FS(config-if-GigabitEthernet 0/1)# aggregateport primary-port FS(config-if-GigabitEthernet 0/1)# end FS# show interface aggregateport 1 ... Aggregate Port Informations: Aggregate Number: 1 Name: "AggregatePort 1"</pre>	

	Members: (count=1) Primary Port: GigabitEthernet 0/1 GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.7 hash-disturb

	Use this command to configure HASH disturbance. Use the no form of this command to restore the default setting.	
	hash-disturb <i>string</i>	
	no hash-disturb	
Parameter Description	Parameter	Description
	<i>string</i>	HASH disturbance.
Defaults	This function is disabled by default.	
Command Mode	Enhanced template configuration mode	
Usage Guide	You can configure this function if you want to balance packets of the same type among multiple devices of the same type.	
Configuration Examples	The following example configures the HASH disturbance. <pre> FS# configure terminal FS(config)#load-balance-profile FS(config-load-balance-profile)# FS(config-load-balance-profile)#hash-disturb A FS(config-load-balance-profile)# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 hash-symmetrical

	Use this command to configure HASH symmetry. Use the no form of this command to restore the default setting.	
	hash-symmetrical {ipv4 ipv6 }	
	no hash-symmetrical {ipv4 ipv6 }	
Parameter	Parameter	Description
Description	ipv4	Configures HASH symmetry for IPv4 packets.
	ipv6	Configures HASH symmetry for IPv6 packets.
Defaults	This function is enabled by default.	
Command Mode	Enhanced template configuration mode	
Usage Guide	You can configure this function if you want to specify a link for both the uplink and downlink traffic of packets of the same type.	
Configuration Examples	The following example disables HASH symmetry for IPv6 packets. <pre> FS# configure terminal FS(config)#load-balance-profile FS(config-load-balance-profile)# FS(config-load-balance-profile)#no hash-symmetrical ipv6 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.9 interfaces aggregateport

	Use this command to create the aggregate port or enter interface configuration mode of the aggregate port. Use the no form of this command to restore the default setting.	
	interfaces aggregateport ap-number	
	no interfaces aggregateport ap-number	
Parameter	Parameter	Description
Description	<i>ap-number</i>	Aggregate port number.
Defaults	The aggregate port is not created by default.	
Command	Global configuration mode	

Mode		
Usage Guide	If the aggregate port is created, this command is used to enter the interface configuration mode. Otherwise, this command is used to create the aggregate port and then enter its interface configuration mode.	
Configuration Examples	The following example creates AP 5 and enters its interface configuration mode. <pre>FS# configure terminal FS(config)# interfaces aggregateport 5 FS(config-if-Aggregateport 5)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.10 ipv4 field

	Use this command to configure the IPv4 load balance mode for a specified profile. Use the no form of this command to restore the default setting.	
	ipv4 field [src-ip] [dst-ip] [protocol] [l4-src-port] [l4-dst-port] [vlan]	
	no ipv4 field	
Parameter Description	Parameter	Description
	src-ip	Load balance based on the source IP address of the IPv4 packet.
	dst-ip	Load balance based on the destination IP address of the IPv4 packet.
	protocol	Load balance based on the protocol type of the IPv4 packet.
	l4-src-port	Load balance based on the L4 source port number of the IPv4 packet.
	l4-dst-port	Load balance based on the L4 destination port number of the IPv4 packet.
	vlan	Load balance based on the VLAN ID of the IPv4 packet.
Defaults	The default load balance mode is src-ip and dst-ip .	
Command Mode	Load balance profile configuration mode	
Usage Guide	You need to configure the load balance profile first.	
Configuration Examples	The following example sets the IPv4 load balance mode for profile apl to src-ip. <pre>FS# configure terminal FS(config)# load-balance-profile apl FS(config-load-balance-profile)# ipv4 field src-ip</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.11 ipv6 field

	Use this command to configure the IPv6 load balance mode for a specified profile. Use the no form of this command to restore the default setting.	
	ipv6 field [src-ip] [dst-ip] [protocol] [l4-src-port] [l4-dst-port] [vlan]	
	no ipv6 field	
Parameter Description	Parameter	Description
	src-ip	Load balance based on the source IP addresses of the IPv6 packets.
	dst-ip	Load balance based on the destination IP addresses of the IPv6 packets.
	protocol	Load balance based on the protocol types of the IPv6 packets.
	l4-src-port	Load balance based on the L4 source port numbers of the IPv6 packets.
	l4-dst-port	Load balance based on the L4 destination port numbers of the IPv6 packets.
	vlan	Load balance based on the VLAN ID of the IPv4 packet.
Defaults	The default load balance mode is src-ip and dst-ip .	
Command Mode	Load balance profile configuration mode	
Usage Guide	You need to configure the load balance profile first.	
Configuration Examples	The following example sets the load balance mode of IPv6 packets to src-ip. <pre>FS(config)# load-balance-profile apl FS(config-load-balance-profile)# ipv6 field src-ip</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.12 l2 field

	Use this command to configure the load balance mode of L2 packets for a specified profile. Use the no form of this command to restore the default setting.

	l2 field [src-mac] [dst-mac] [vlan]	
	no l2 field	
Parameter Description	Parameter	Description
	src-mac	Load balance based on the source MAC address of the L2 packet.
	dst-mac	Load balance based on the destination MAC address of the L2 packets.
	vlan	Load balance based on the VLAN ID of the L2 packet.
Defaults	The default load balance mode is src-mac , dst-mac , and vlan .	
Command Mode	Load balance profile configuration mode	
Usage Guide	You need to configure the load balance profile first.	
Configuration Examples	The following example sets the load balance mode of L2 packets to src-mac and src-prot .	
	<pre>FS(config)# load-balance-profile apl FS(config-load-balance-profile)# l2 field src-mac src-port</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.13 lacp individual-port enable

	Use this command to enable the LACP independent port function. Use the no form of this command to restore the default setting.	
	lacp individual-port enable	
	no lacp individual-port enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the LACP independent port function is disabled.	
Command Mode	Interface configuration mode	
Usage Guide	(Optional) Perform this operation when the LACP member port cannot perform LACP negotiation and need to be changed to a common physical port. After this function is enabled, the member port becomes an independent port (a common physical port) if LACP negotiation fails because the port does not receive LACP packets from the peer end within the set time-out	

	period.				
Configuration Examples	This example shows how to enable the independent port function for GigabitEthernet 0/1. <pre> FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# port-group 1 mode active FS(config-if-GigabitEthernet 0/1)# lacp individual enable FS(config-if-GigabitEthernet 0/1)# end FS# show interface aggregateport 1 ... Aggregate Port Informations: Aggregate Number: 1 Name: "AggregatePort 1" Members: (count=1) Primary Port: GigabitEthernet 0/1 GigabitEthernet 0/1 Link Status: Up Lacp Status: individual ... </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

3.14 lacp port-priority

	Use this command to set the priority of the LACP AP member port. Use the no form of this command to restore the default setting.	
	lacp port-priority <i>port-priority</i>	
	no lacp port-priority	
Parameter Description	Parameter	Description
	<i>port-priority</i>	The LACP port priority, in the range from 0 to 65535.
Defaults	The default is 32768.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	This example sets the LACP port priority of interface Gi0/1 to 4096. <pre> FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# lacp port-priority 4096 </pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.15 lacp short-timeout

	Use this command to configure the short-timeout mode for the LACP AP member port. Use the no form of this command to restore the default setting.	
	lacp short-timeout	
	no lacp short-timeout	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default is long-timeout mode.	
Command Mode	Interface configuration mode	
Usage Guide	In long-timeout mode, the port sends an LACP packet every 30 seconds. If the packet is not received in 90 seconds, the connection times out. In short-timeout mode, the port sends an LACP packet every 1 second. If the packet is not received in 3 seconds, the connection times out.	
Configuration Examples	The following example configures the short-timeout mode for the LACP AP member port. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# lacp short-timeout</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.16 lacp system-priority

	Use this command to set the LACP system priority. Use the no form of this command to restore the default setting.	
	lacp system-priority <i>system-priority</i>	

	no lacp system-priority	
Parameter Description	Parameter	Description
	<i>system-priority</i>	The LACP system priority, in the range from 0 to 65535.
Defaults	The default is 32768.	
Command Mode	Global configuration mode.	
Usage Guide		
Configuration Examples	The following example sets the LACP system priority to 4096. <pre>FS(config)# lacp system-priority 4096</pre>	
Related Commands	Command	Description
	port-group <i>key</i> mode { active passive }	Enables the LACP on the port and specifies the aggregation group ID and operation mode.
	lacp port-priority	Sets the LACP port priority.
Platform Description	N/A	

3.17 load-balance-profile

	Use this command to rename a load balance enhanced profile and apply the profile. Use the default form of this command to restore the default setting.	
	load-balance-profile <i>profile-name</i>	
	no load-balance-profile <i>profile-name</i>	
	no load-balance-profile	
Parameter Description	Parameter	Description
	<i>profile-name</i>	Specifies the profile name, which contains up to 31 characters.
Defaults	The default <i>profile-name</i> is default.	
Command Mode	Global configuration mode.	
Usage Guide	By default, the device is configured with an enhanced profile named default. Use the load-balance-profile default command to enter the enhanced profile configuration mode. You can change the profile name by using	

	the load-balance-profile <i>profile-name</i> command.					
Configuration Examples	The following example creates a load balance profile named apl . <pre>FS(config)# load-balance-profile apl Warning: The profile default has been used, and this command will rename it. Continue? [Y/N]:y FS(config-load-balance-profile)#</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

3.18 port-group

	Use this command to assign a physical interface to be a member port of a static aggregate port or an LACP aggregate port. Use the no form of this command to restore the default setting.	
	port-group <i>port-group-number</i>	
	port-group <i>key-number</i> mode { active passive }	
	no port-group	
Parameter	Parameter	Description
	Description	<i>port-group-number</i>
	<i>key-number</i>	Member group ID of an LACP aggregate port, the interface number of the LACP aggregate port.
	active	Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
	passive	Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation.
Defaults	By default, the physical port does not belong to any aggregate port.	
Command Mode	Interface configuration mode.	
Usage Guide	All the members of an aggregate port belong to a VLAN or configured to be trunk ports. The ports belonging to different native VLANs cannot form an aggregate port.	
Configuration Examples	The following example specifies the Ethernet interface 1/3 as a member of the static AP 3. FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)# port-group 3 The following example specifies the Ethernet interface 2/3 as a member of the LACP AP4 and set the aggregation mode to active.	

	FS(config)# interface gigabitethernet 2/3 FS(config-if-GigabitEthernet 2/3)# port-group 4 mode active	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.19 show aggregateport

	Use this command to display the aggregate port configuration.					
	show aggregateport <i>aggregate-port-number</i> [load-balance summary]					
Parameter Description	Parameter			Description		
	<i>aggregate-port-number</i>			Number of the aggregate port.		
	load-balance			Displays the load-balance algorithm on the aggregate port.		
	summary			Displays the summary of the aggregate port.		
Defaults	N/A					
Command Mode	Any mode					
Usage Guide	If the aggregate port number is not specified, all the aggregate port information will be displayed.					
Configuration Examples	The following example displays the aggregate port configuration.					
	FS# show aggregateport 1 summary					
	AggregatePort	MaxPorts	SwitchPort	Mode	Load balance	Ports
	Ag1	8	Enabled	ACCESS	dst-mac	Gi0/2

The following example displays the configuration information of **load-balance** globally.

```
FS#show aggregateport load-balance
```

```
Load-balance      : Source MAC and Destination MAC
```

```
Hash-elasticity : enable
```

```
Algorithm mode
```

```
current: 3, default: 0
```

```
Hash-disturb(Expert Mode):
```

```
current seed: 1, offset 0.
```

```
default seed: 0, offset 0.
```

Field	Description
Load-balance	Indicates global load balancing mode.
Hash-elasticity	Indicates whether Hash elasticity is enabled.
Algorithm mode	Indicates Hash load-balancing algorithm mode.
Hash-disturb(Expert Mode)	Indicates the seed and offset values of Hash disturbance. Not all models are able to display this such information. "Current" stands for the current values, and "default" for the default ones.

Related Commands	Command	Description
	aggregateport load-balance	Configures a load-balance algorithm of AP.
Platform Description	N/A	

3.20 show aggregateport capacity

Use this command to display the AP capacity mode and the AP number.

```
show aggregateport capacity
```

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the AP capacity mode and the AP number. <pre>FS# show aggregateport capacity</pre> AggregatePort Capacity Information: Configuration Capacity Mode: 128*16.	

	Effective Capacity Mode : 256*8. Available Capacity : 128*8. Total Number: 128, Used: 1, Available: 127.	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.21 show lacp summary

	Use this command to display the LACP aggregation information.	
	show lacp summary [<i>key-number</i>]	
Parameter Description	Parameter	Description
	<i>key-number</i>	Specifies the aggregation group id to show.
Defaults	N/A	
Command Mode	Any mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the LACP aggregation information. <pre> FS(config)# show lacp summary 3 System Id:32768, 00d0.f8fb.0002 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State ----- Gi0/1 SA bndl 4096 0x3 0x1 0x3d Gi0/2 SA bndl 4096 0x3 0x2 0x3d Gi0/3 SA bndl 4096 0x3 0x3 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State ----- </pre>	

	Gi0/1	SA	61440	00d0.f800.0002	0x3	0x1	0x3d
	Gi0/2	SA	61440	00d0.f800.0002	0x3	0x2	0x3d
	Gi0/3	SA	61440	00d0.f800.0002	0x3	0x3	0x3d
Related Commands	Command			Description			
	port-group <i>key mode</i>			Enables the LACP on the port and specifies the aggregation group ID and operation mode.			
Platform Description	N/A						

3.22 show load-balance-profile

	Use this command to display the enhanced profile.	
	show load-balance-profile [<i>profile-name</i>]	
Parameter	Parameter	Description
Description	<i>profile-name</i>	Specifies the profile name.
Defaults	-	
Command Mode	Any mode.	
Usage Guide	All enhanced profiles are displayed if the profile name is not specified.	
Configuration Examples	The following example displays the enhanced profile of module0. <pre>FS# show load-balance-profile module0 Load-balance-profile: module0 Packet Hash Field: IPv4: src-ip dst-ip IPv6: src-ip dst-ip L2 : src-mac dst-mac vlan</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4 VLAN Commands

4.1 add

	Use this command to add one or a group Access interface into current VLAN. Use the no or default form of the command to remove the Access interface.	
	add interface { <i>interface-id</i> range <i>interface-range</i> }	
	no add interface { <i>interface-id</i> range <i>interface-range</i> }	
	default add interface { <i>interface-id</i> range <i>interface-range</i> }	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Layer-2 Ethernet interface or layer-2 AP port.
	range <i>interface-range</i>	Range of the Layer-2 Ethernet interface or layer-2 AP port.
Defaults	All layer-2 Ethernet interfaces are in the VLAN1.	
Command Mode	VLAN configuration mode.	
Usage Guide	This command is only valid for the access port. The configuration of this command is the same as specifying the VLAN to which interface belongs in the interface configuration mode (that is the switchport access vlan <i>vlan-id</i> command). For the two commands of adding the interface to the VLAN, the command configured later will overwrite the one configured before and take effect. The configuration of adding the layer-2 AP into current VLAN through this command will only take effect for the layer-2 AP port, but not for the member port of the layer-2 AP port.	
Configuration Examples	The following example adds the interface GigabitEthernet 0/10 to VLAN20. <pre> FS# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface GigabitEthernet 0/10 FS# show interface GigabitEthernet 0/10 switchport Interface Switchport Mode Access Native Protected VLAN lists ----- - GigabitEthernet 0/10 enabled ACCESS 20 1 Disabled ALL </pre> The following example adds the interface range GigabitEthernet 0/1-10 to VLAN200. <pre> FS# configure terminal SwitchA(config)#vlan 200 SwitchA(config-vlan)#add interface range GigabitEthernet 0/1-10 FS# show vlan SwitchA#show vlan VLAN Name Status ----- - </pre>	

	<pre>1 VLAN0001 STATIC Gi0/11,Gi0/12,Gi0/13,Gi0/14,Gi0/15, Gi0/16,Gi0/17,Gi0/18,Gi0/19,Gi0/20,Gi0/21, Gi0/22, Gi0/23, Gi0/24 200 VLAN0200 STATIC Gi0/1,Gi0/2,Gi0/3,Gi0/4,Gi0/5, Gi0/6,Gi0/7,Gi0/8,Gi0/9,Gi0/10</pre> The following example adds the AggregatePort10 to VLAN20. <pre>FS# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface aggregateport 10 FS# show interface aggregateport 10 switchport</pre> <table><tr><th>Interface</th><th>Switchport</th><th>Mode</th><th>Access</th><th>Native</th><th>Protected</th><th>VLAN lists</th></tr><tr><td>AggregatePort 10</td><td>enabled</td><td>ACCESS</td><td>20</td><td>1</td><td>Disabled</td><td>ALL</td></tr></table>		Interface	Switchport	Mode	Access	Native	Protected	VLAN lists	AggregatePort 10	enabled	ACCESS	20	1	Disabled	ALL
Interface	Switchport	Mode	Access	Native	Protected	VLAN lists										
AggregatePort 10	enabled	ACCESS	20	1	Disabled	ALL										
Related Commands	Command	Description														
	show interface <i>interface-id</i> switchport	Displays the layer-2 interfaces.														
Platform Description	N/A															

4.2 name

	Use this command to specify the name of a VLAN. Use the no or default form of this command to restore the default setting.	
	name <i>vlan-name</i>	
	no name	
	default name	
Parameter Description	Parameter	Description
	<i>vlan-name</i>	VLAN name
Defaults	The default name of a VLAN is the combination of "VLAN" and VLAN ID, for example, the default name of the VLAN 2 is "VLAN0002".	
Command Mode	VLAN configuration Mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the name of VLAN to 10. <pre>FS(config)# vlan 10 FS(config-vlan)# name vlan10</pre>	

Related Commands	Command	Description
	show vlan	Displays member ports of the VLAN.
Platform Description	N/A	

4.3 show vlan

	Use this command to display member ports of the VLAN.							
	show vlan [id <i>vlan-id</i>]							
Parameter Description	Parameter	Description						
	<i>vlan-id</i>	VLAN ID						
Defaults	N/A							
Command Mode	All modes							
Usage Guide	N/A							
Configuration Examples	The following command displays the status of VLAN 1. <pre>FS(config-vlan)#show vlan id 20</pre> <table> <tr> <th>VLAN Name</th><th>Status</th><th>Ports</th></tr> <tr> <td>20 VLAN0020</td><td>STATIC</td><td>Gi0/1</td></tr> </table>		VLAN Name	Status	Ports	20 VLAN0020	STATIC	Gi0/1
VLAN Name	Status	Ports						
20 VLAN0020	STATIC	Gi0/1						
Related Commands	Command	Description						
	name	VLAN name.						
	switchport access	Adds the interface to a VLAN.						
Platform Description	N/A							

4.4 switchport access

	Use this command to configure an interface as a static access port and assign it to a VLAN. Use the no or default form of the command to assign the port to the default VLAN.

	switchport access vlan <i>vlan-id</i>	
	no switchport access vlan	
	default switchport access vlan	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN ID at which the port to be added.
Defaults	By default, the switch port is an access port and the VLAN is VLAN 1.	
Command Mode	Interface configuration mode.	
Usage Guide	Enter one VLAN ID. The system will create a new one and add the interface to the VLAN if you enter a new VLAN ID. If the VLAN ID already exists, the command adds the port to the VLAN. If the port is a trunk port, the operation does not take effect.	
Configuration Examples	FS(config)# interface gigabitethernet 1/1 FS(config-if)# switchport access vlan 2	
Related Commands	Command	Description
	switchport mode	Specifies the interface as Layer 2 mode (switch port mode).
	switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.
Platform Description	N/A	

4.5 switchport hybrid allowed

	Use this command to add the port to the VLAN or remove the port from the VLAN, Use the no or default form of this command to restore the default setting.	
	switchport hybrid allowed vlan { { [add only] tagged <i>vlist</i> [add] untagged <i>vlist</i> } remove <i>vlist</i> }	
	no switchport hybrid allowed vlan	
	default switchport hybrid allowed vlan	
Parameter Description	Parameter	Description
	add	Adds the port to the VLAN.
	only	Adds the port to the VLAN and removes the port from the VLANs not on the VLAN list.
	tagged	Adds the port to the VLAN and the VLAN packets going out on the port are

		tagged with VLAN ID.
	untagged	Adds the port to the VLAN and the VLAN packets going out on the port are not tagged with VLAN ID.
	remove	Removes the port from the VLAN.
	<i>vlist</i>	Specifies the VLAN.
Defaults	By default, the hybrid port is in all VLANs. All VLAN packets (except native VLAN packets) going out on the port are tagged with VLAN ID. Native VLAN packets are not tagged with VLAN ID.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example adds the hybrid port to VLAN 20 and VLAN 30 and the VLAN packets going out on the port are not tagged with VLAN ID. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# switchport mode hybrid FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged 20 FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan add untagged 30</pre> The following example adds the hybrid port to VLAN 40 and VLAN 50 and the VLAN packets going out on the port are tagged with VLAN ID, <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#switchport mode hybrid FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged 40 FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged 50</pre> The following example removes the hybrid port from VLAN 20. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#switchport mode hybrid FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan remove 20</pre> The following example adds the hybrid port to VLAN 20 and deletes all the other VLANs. The VLAN packets going out on the port are tagged with VLAN ID. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#switchport mode hybrid FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan only tagged 20</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.6 switchport hybrid native

	Use this command to configure the native VLAN for the hybrid port. Use the no or default form of this command to restore the default setting.
	switchport hybrid native vlan <i>vlan-id</i>
	no switchport hybrid native vlan

	default switchport hybrid native vlan	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	Configures the native VLAN for the hybrid port.
Defaults	The default is VLAN 1.	
Command Mode	Interface configuration mode	
Usage Guide	Native VLAN packets going out on the hybrid port are not tagged with VLAN ID. Packets not tagged with VLAN ID coming in on the hybrid port are taken as native VLAN packets.	
Configuration Examples	The following example configures VLAN 20 as the native VLAN for hybrid port GigabitEthernet 0/1. FS(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#switchport mode hybrid FS(config-if-GigabitEthernet 0/1)#switchport hybrid native vlan 20	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.7 switchport mode

	Use this command to specify a L2 interface (switch port) mode. You can specify this interface to be an access port or a trunk port. Use the no or default form of this command to restore the default setting.	
	switchport mode { access trunk hybrid uplink }	
	no switchport mode	
	default switchport mode	
Parameter Description	Parameter	Description
	access	Configures the switch port as an access port.
	trunk	Configures the switch port as a trunk port.
	hybrid	Configures the switch port as a hybrid port.
	uplink	Configures the switch port as an uplink port.
Defaults	By default, the switch port is an access port.	
Command Mode	Interface configuration mode.	

Usage Guide	If a switch port is an access port, the port can be added only to one VLAN. You can run the switchport access vlan command to specify the VLAN to which the port belongs. If a switch port is a trunk port, the port is added to all VLANs by default. You can also run the switchport trunk allowed command to add the port to or remove the port from a specified VLAN. If a switch port is an uplink port, the port is added to all VLANs by default. Different from the trunk port, the uplink port sends packets with a tag carried, that is, the tag of packets from default VLANs will not be deleted. You can run the switchport trunk allowed command to add the port to or remove the port from a specified VLAN. If a switch port is a hybrid port, the port is added to all VLANs by default. Different from a trunk port, a hybrid port can be added to a VLAN in tag or untag mode by running the switchport hybrid allowed command.	
Configuration Examples	The following example configures port 1 as an access port. <pre>FS(config)#int g 0/1 FS(config-if-GigabitEthernet 0/1)#switchport mode access</pre> The following example configures port 1 as a trunk port. <pre>FS(config)#int g 0/1 FS(config-if-GigabitEthernet 0/1)# switchport mode trunk</pre> The following example configures port 1 as an uplink port. <pre>FS(config)#int g 0/1 FS(config-if-GigabitEthernet 0/1)# switchport mode uplink</pre> The following example configures port 1 as a hybrid port. <pre>FS(config)#int g 0/1 FS(config-if-GigabitEthernet 0/1)# switchport mode hybrid</pre>	
Related Commands	Command	Description
	switchport access	Configures an interface as a statics access port and assigns it to a VLAN.
	switchport trunk	Specifies a native VLAN and the allowed-VLAN list for the trunkport.
Platform Description	N/A	

4.8 switchport trunk allowed vlan

	Use this command to add the trunk/uplink port to the VLAN or remove a trunk/uplink port from the VLAN. Use the no or default form of the command to restore the default setting.
	switchport trunk allowed vlan { all { add vlan-list remove vlan-list except vlan-list only vlan-list } }
	no switchport trunk allowed vlan
	default switchport trunk allowed vlan

Parameter Description	Parameter	Description
	all	Adds the trunk/uplink port to all VLANs.
	add	Adds the trunk/uplink port to the VLAN.
	remove	Removes the trunk/uplink port from the VLAN port.
	except	Removes the trunk/uplink port from the VLAN and adds the port to all the other VLANs.
	only	Adds the trunk/uplink port to the specified VLAN and removes the port from the VLANs not on the VLAN list.
	<i>vlan-list</i>	Specifies the VLAN.
Defaults	The trunk/unlink port is in all VLANs by default.	
Command Mode	Interface configuration mode.	
Usage Guide	A trunk/uplink port transmits all VLAN (1-4094) data by default. You can block some VLAN data by configuring this command. Use the show interfaces command to display configuration.	
Configuration Examples	The following example removes trunk port GigabitEthernet 0/10 from VLAN 2. <pre>FS(config)# interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport mode trunk FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 2</pre> The following example removes trunk port GigabitEthernet 0/10 from VLAN 2. <pre>FS(config)# interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10</pre> The following example removes uplink port GigabitEthernet 0/10 from VLAN 10. <pre>FS(config)# interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport mode uplink FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 10</pre> The following example adds uplink port GigabitEthernet 0/10 to all VLANs except VLAN10. <pre>FS(config)# interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.9 switchport trunk native vlan

	Use this command to configure the native VLAN for the trunk/uplink port. Use the no or default form of this command to restore the default setting.	
	switchport trunk native vlan <i>vlan-id</i>	
	no switchport trunk native vlan	
	default switchport trunk native vlan	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	Native VLAN ID.
Defaults	By default, the native VLAN for the trunk/uplink port is VLAN 1.	
Command Mode	Interface configuration mode	
Usage Guide	After this function is enabled, packets not tagged with VLAN ID are taken as native VLAN packets. Tags are removed from native VLAN packets going out on the trunk port.	
Configuration Examples	The following example configures VLAN 10 as the native VLAN for trunk port GigabitEthernet 0/10. <pre>FS(config)#interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport mode trunk FS(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10</pre> The following example configures VLAN 10 as the native VLAN for uplink port GigabitEthernet 0/10. <pre>FS(config)#interface gigabitEthernet 0/10 FS(config-if-GigabitEthernet 0/10)# switchport mode uplink FS(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.10 vlan

	Use this command to enter the VLAN configuration mode. Use the no or default form of this command to restore the default setting.	
	vlan { <i>vlan-id</i> range <i>vlan-range</i> }	
	no vlan { <i>vlan-id</i> range <i>vlan-range</i> }	
	default vlan { <i>vlan-id</i> range <i>vlan-range</i> }	

Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID Default VLAN (VLAN 1) cannot be removed.
	<i>vlan-range</i>	VLAN ID range.
Defaults	The default is static VLAN.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example creates VLAN 10.	
	<pre>FS(config)# vlan 10 FS(config-vlan)#</pre>	
Related Commands	Command	Description
	show vlan	Displays member ports of the VLAN.
Platform Description	N/A	

5 Super-VLAN Commands

5.1 proxy-arp

	Use this command to enable the proxy ARP function for a VLAN. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	proxy-arp	
	no proxy-arp	
	default proxy-arp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	VLAN configuration Mode.	
Usage Guide	Super VLAN and sub VLAN must be both enabled with proxy ARP.	
Configuration Examples	The following example enables the proxy ARP function for VLAN 3. <pre>FS(config)# vlan 3 FS(config-vlan)# proxy-arp</pre> The following example disables the proxy ARP function for VLAN 3. <pre>FS(config)# vlan 3 FS(config-vlan)# no proxy-arp</pre>	
Related Commands	Command	Description
	show supervlan	Displays the super VLAN information.
Platform Description	N/A	

5.2 show supervlan

	Use this command to display the configuration of the super VLAN and its sub VLANs.	
	show supervlan	
	show supervlan <i>vlan-id</i>	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID

Defaults	N/A																																																						
Command Mode	Any mode																																																						
Usage Guide	N/A																																																						
Configuration Examples	The following example displays the configuration of super VLAN 2. SwitchA(config-if-range)# show supervlan 2 <table><thead><tr><th>supervlan id</th><th>supervlan arp-proxy</th><th>subvlan id</th><th>subvlan arp-proxy</th><th>subvlan ip range</th></tr></thead><tbody><tr><td>2</td><td>ON</td><td>10</td><td>ON</td><td>192.168.196.10 - 192.168.196.50</td></tr><tr><td></td><td></td><td>20</td><td>ON</td><td>192.168.196.60 - 192.168.196.100</td></tr><tr><td></td><td></td><td>30</td><td>ON</td><td>192.168.196.110 - 192.168.196.150</td></tr></tbody></table> following example displays the configuration of all super VLANs. SwitchA(config-if-range)# show supervlan <table><thead><tr><th>supervlan id</th><th>supervlan arp-proxy</th><th>subvlan id</th><th>subvlan arp-proxy</th><th>subvlan ip range</th></tr></thead><tbody><tr><td>2</td><td>ON</td><td>10</td><td>ON</td><td>192.168.196.10 - 192.168.196.50</td></tr><tr><td></td><td></td><td>20</td><td>ON</td><td>192.168.196.60 - 192.168.196.100</td></tr><tr><td></td><td></td><td>30</td><td>ON</td><td>192.168.196.110 - 192.168.196.150</td></tr><tr><td>6</td><td>ON</td><td>7</td><td>ON</td><td></td></tr><tr><td></td><td></td><td>8</td><td>ON</td><td></td></tr></tbody></table>					supervlan id	supervlan arp-proxy	subvlan id	subvlan arp-proxy	subvlan ip range	2	ON	10	ON	192.168.196.10 - 192.168.196.50			20	ON	192.168.196.60 - 192.168.196.100			30	ON	192.168.196.110 - 192.168.196.150	supervlan id	supervlan arp-proxy	subvlan id	subvlan arp-proxy	subvlan ip range	2	ON	10	ON	192.168.196.10 - 192.168.196.50			20	ON	192.168.196.60 - 192.168.196.100			30	ON	192.168.196.110 - 192.168.196.150	6	ON	7	ON				8	ON	
supervlan id	supervlan arp-proxy	subvlan id	subvlan arp-proxy	subvlan ip range																																																			
2	ON	10	ON	192.168.196.10 - 192.168.196.50																																																			
		20	ON	192.168.196.60 - 192.168.196.100																																																			
		30	ON	192.168.196.110 - 192.168.196.150																																																			
supervlan id	supervlan arp-proxy	subvlan id	subvlan arp-proxy	subvlan ip range																																																			
2	ON	10	ON	192.168.196.10 - 192.168.196.50																																																			
		20	ON	192.168.196.60 - 192.168.196.100																																																			
		30	ON	192.168.196.110 - 192.168.196.150																																																			
6	ON	7	ON																																																				
		8	ON																																																				
Related Commands	Command			Description																																																			
	N/A			N/A																																																			
Platform Description	N/A																																																						

5.3 subvlan

	Use this command to set the sub VLAN for the super VLAN. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	subvlan <i>vlan-id-list</i>	
	no subvlan [<i>vlan-id-list</i>]	
	default subvlan [<i>vlan-id-list</i>]	
Parameter Description	Parameter	Description
	<i>vlan-id-list</i>	Sub VLAN ID of the VLAN. Multiple VLANs are supported.

Defaults	No super VLAN is set by default.				
Command Mode	VLAN configuration Mode.				
Usage Guide	Use the no subvlan command to delete all sub VLANs of this super VLAN.				
Configuration Examples	The following example sets the sub VLAN. <pre>SwitchA(config)#vlan 2 SwitchA(config-vlan)#supervlan SwitchA(config-vlan)#subvlan 10,20,30</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show supervlan</td><td>Displays the super VLAN information.</td></tr> </table>	Command	Description	show supervlan	Displays the super VLAN information.
Command	Description				
show supervlan	Displays the super VLAN information.				
Platform Description	N/A				

5.4 subvlan-address-range

	Use this command to set the IP address range of the sub VLAN. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	subvlan-address-range <i>start-ip end-ip</i>	
	no subvlan-address-range	
	default subvlan-address-range	
Parameter Description	Parameter	Description
	<i>start-ip</i>	The start IP address of this sub VLAN
	<i>end-ip</i>	The end IP address of this sub VLAN
Defaults	No IP address range is set by default.	
Command Mode	VLAN configuration Mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the IP address range for the sub VLAN. <pre>FS(config)# vlan 2 FS(config-vlan)#subvlan-address-range 192.168.23.1 192.168.23.5</pre>	

Related Commands	Command	Description
	show supervlan	Displays the super VLAN information.
Platform Description	N/A	

5.5 supervlan

	Use this command to set the VLAN as a super VLAN. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	supervlan	
	no supervlan	
	default supervlan	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No super VLAN is set by default.	
Command Mode	VLAN configuration Mode.	
Usage Guide	No physical port can be added to a super VLAN.	
Configuration Examples	The following example configures a Sub VLAN. FS(config)# vlan 2 FS(config-vlan)#supervlan	
Related Commands	Command	Description
	show supervlan	Displays the super VLAN information.
Platform Description	N/A	

6 Private VLAN Commands

6.1 debug bridge pvlan

	Use this command to enable private VLAN debugging. Use the no or default form of this command to restore the default setting.	
	debug bridge pvlan	
	no debug bridge pvlan	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Debugging is disabled by default.	
Command Mode	Privileged EXEC mode	
Usage Guide	Debugging information includes error and prompt messages appearing during private VLAN configuration. This command can be used to troubleshoot VLAN and interface configuration failure.  With private VLAN debugging enabled, all super VLAN configuration and packet processing on SVI is displayed.  Debugging information helps troubleshooting and fault location.	
Configuration Examples	The following example enables private VLAN debugging. <pre>FS# debug bridge pvlan</pre> The following example disables private VLAN debugging. <pre>FS# no debug bridge pvlan</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.2 private-vlan

	Use this command to configure the private VLAN feature. Use the no or default form of this command to restore the default setting.	
	private-vlan { community isolated primary }	
	no private-vlan { community isolated primary }	
	default private-vlan { community isolated primary }	

Parameter Description	Parameter	Description
	community	Sets the community VLAN.
	isolated	Sets the isolated VLAN.
	primary	Sets the primary VLAN.
Defaults	No private VLAN feature is configured by default.	
Command Mode	VLAN configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example configures the private VLAN feature. <pre>FS(config)#vlan 90 FS(config-vlan)#private-vlan primary FS(config-vlan)#vlan 91 FS(config-vlan)#private-vlan isolated FS(config-vlan)#vlan 92 FS(config-vlan)#private-vlan community</pre> The following example disables the private VLAN feature using the no private-vlan command. <pre>FS(config)#vlan 90 FS(config-vlan)#no private-vlan primary FS(config-vlan)#vlan 91 FS(config-vlan)#no private-vlan isolated FS(config-vlan)#vlan 92 FS(config-vlan)#no private-vlan community</pre> The following example disables the private VLAN feature using the default private-vlan command. <pre>FS(config)#vlan 90 FS(config-vlan)#default private-vlan primary FS(config-vlan)#vlan 91 FS(config-vlan)#default private-vlan isolated FS(config-vlan)#vlan 92 FS(config-vlan)#default private-vlan community</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.3 private-vlan association

	Use this command to associate the secondary VLAN with the primary VLAN on layer 2. Use the no or default form of this command to restore the default setting.	
	private-vlan association { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	
	no private-vlan association	
	default private-vlan association	
Parameter Description	Parameter	Description
	<i>svlist</i>	The secondary VLAN list
	add <i>svlist</i>	Adds the associated secondary VLAN.
	remove <i>svlist</i>	Removes the associated secondary VLAN.
Defaults	This function is disabled by default.	
Command Mode	VLAN configuration Mode.	
Usage Guide	N/A	
Configuration Examples	The following example associates the secondary VLAN with the primary VLAN on layer 2. <pre>FS(config)# vlan 22 FS(config-vlan)# private-vlan association add 24-26</pre>	
	The following example removes the association between the secondary VLAN with the primary VLAN. <pre>FS(config)# vlan 22 FS(config-vlan)# private-vlan association remove 24</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.4 private-vlan mapping

	Use this command to associate the secondary VLAN with the primary VLAN on layer 3. Use the no or default form of this command to restore the default setting.	
	private-vlan mapping { <i>svlist</i> add <i>svlist</i> remove <i>svlist</i> }	
	no private-vlan mapping	
	default private-vlan mapping	

Parameter Description	Parameter	Description
	<i>svlist</i>	Secondary VLAN list.
	add <i>svlist</i>	Adds the associated secondary VLAN.
	remove <i>svlist</i>	Removes the associated secondary VLAN.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example associates the secondary VLAN with the primary VLAN on layer 3. <pre>FS(config)# interface vlan 22 FS(config-if)# private-vlan mapping add 24-26</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.5 show vlan private-vlan

	Use this command to display the private VLAN configuration.	
	show vlan private-vlan [community primary isolated]	
	Use this command to display all the private VLANs configuration. show vlan private-vlan	
Parameter Description	Parameter	Description
	primary	Displays the primary VLAN information.
	community	Displays the community VLAN information.
	isolated	Displays the isolated VLAN information.
Defaults	N/A	
Command Mode	All modes	
Usage Guide	N/A	

Configuration Examples	The following example displays the private VLAN configuration.					
	FS# show vlan private-vlan					
	VLAN	Type	Status	Routed	Ports	Associated VLANs

	30	primary	inactive	Enabled		
	31	isolated	inactive	Disabled		No Association
	90	primary	active	Disabled		91-92
	91	isolated	active	Disabled		90
	92	community	active	Disabled	Gi0/1	90
Related Commands	Command			Description		
	N/A			N/A		
Platform Description	N/A					

6.6 switchport mode private-vlan

	Use this command to declare the private VLAN mode of the interface. Use the no or default form of this command to restore the default setting.	
	switchport mode private-vlan { host promiscuous }	
	no switchport mode	
	default switchport mode	
Parameter Description	Parameter	Description
	host	Host mode of the private VLAN
	promiscuous	Promiscuous mode of the private VLAN
Defaults	The port is an access port by default.	
Command Mode	Interface configuration mode.	
Usage Guide	Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode. The port mode must be configured as the promiscuous mode.	
Configuration Examples	The following example applies the private host mode to the interface. <pre>FS(config)# interface gigabitEthernet0/2 FS(config-if)# switchport mode private-vlan host</pre>	

	The following example applies the promiscuous mode to the interface. <pre>FS(config)# interface gigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)#sw mode private-vlan promiscuous</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.7 switchport private-vlan association trunk

	Use this command to associate the trunk port in the private VLAN mode, which is associated with the primary VLAN and the secondary VLAN. Use the no or default form of this command to restore the default settings.	
	switchport private-vlan association trunk <i>p_vid s_vid</i>	
	no switchport private-vlan association trunk default switchport private-vlan association trunk <i>p_vid s_vid</i>	
Parameter Description	Parameter	Description
	<i>p_vid</i>	Primary VID.
	<i>s_vid</i>	Secondary VID
	no	Deletes the host port from the private VLAN.
Defaults	By default, it is trunk port.	
Command Mode	Interface configuration mode.	
Usage Guide	The associated PVLAN must be a VLAN pair on which Layer-2 association is performed. The interface must work in Trunk port mode. One Trunk port can be associated with multiple PVLAN pairs.	
Configuration Examples	The following example configures a Trunk port, and associates it with a layer 2 port and private VLAN. <pre>FS(config)# interface gigabitEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# switchport private-vlan association trunk 202 203</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.8 switchport private-vlan host-association

	Use this command to associate the primary VLAN, which is associated with the private VLAN mode of the interface, with the secondary VLAN. Use the no or default form of this command to restore the default setting.	
	switchport private-vlan host-association <i>p_vid s_vid</i>	
	no switchport private-vlan host-association	
	default switchport private-vlan host-association	
Parameter Description	Parameter	Description
	<i>p_vid</i>	Primary VID.
	<i>s_vid</i>	Secondary VID
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	Before a port is configured as an isolated port or promiscuous port, and the port mode must be configured as the host port mode. Whether a port is configured as an isolated port or community port depends on the <i>s_vid</i> parameter. <i>p_vid</i> and <i>s_vid</i> must be respectively the IDs of the primary VLAN and secondary VLAN in a PVLAN pair, on which Layer-2 association is performed. One host port can be associated with only one PVLAN pair.	
Configuration Examples	The following example associates the secondary VLAN with the primary VLAN on the host port. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if)# switchport mode private-vlan host FS(config-if)# switchport private-vlan host-association 22 23 FS(config-if)# default switchport private-vlan host-association FS(config-if)# switchport private-vlan host-association 22 25</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.9 switchport private-vlan mapping

	Use this command to configure the secondary VLAN for the promiscuous port. Use the no or default form of this command to restore the default setting.
	switchport private-vlan mapping <i>p_vid { svlist add svlist remove svlist }</i>

	no switchport private-vlan mapping	
	default switchport private-vlan mapping	
Parameter Description	Parameter	Description
	<i>p_vid</i>	Indicates the primary VLAN ID in a PVLAN pair.
	<i>svlist</i>	Indicates the secondary VLAN associated with a promiscuous port. Layer-2 association must be performed between it and <i>p_vid</i> .
	add	Adds a secondary VLAN to be associated with a port.
	remove	Cancels the secondary VLAN associated with a port.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	The port mode must be configured as the promiscuous mode. Layer-2 association must be performed between the primary and secondary VLAN.	
Configuration Examples	The following example configures the secondary VLAN for the promiscuous port. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if)# switchport mode private-vlan promiscuous FS(config-if)# switchport private-vlan mapping 22 add 23-25</pre>	
Related Commands	Command	Description
	show vlan private-vlan	N/A
Platform Description	N/A	

6.10 switchport private-vlan promiscuous trunk

	Use this command to configure the ports as a promiscuous trunk port, which is associated with the L2 port and the private VLAN. Multiple pairs are allowed to associate. Use the no or default form of this command to restore the default settings.	
	switchport private-vlan promiscuous trunk <i>p_vid_s_list</i>	
	no switchport private-vlan promiscuous trunk <i>p_vid_s_list</i>	
Parameter Description	Parameter	Description
	<i>p_vid</i>	Primary VID

	<i>svlist</i>	Secondary VLAN list.
	no	Removes all the relationships between the layer-2 ports and private VLANs.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	The port mode must be a Trunk port. Layer-2 association must be performed between the primary and secondary VLAN.	
Configuration Examples	<pre>FS(config)# interface gigabitEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# switchport private-vlan promiscuous trunk 202 203</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7 MSTP Commands

7.1 bpdu src-mac-check

	Use this command to enable the BPDU source MAC address check function on the interface. Use the no form of this command to restore the default setting.	
	bpdu src-mac-check <i>H.H.H</i>	
	no bpdu src-mac-check	
Parameter Description	Parameter	Description
	<i>H.H.H</i>	Indicates that only the BPDU messages from this MAC address are received.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	BPDU source MAC address check prevents BPDU packets from maliciously attacking switches and causing MSTP abnormal. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check to receive BPDU packets sent only by the peer switch and discard all other BPDU packets, thereby preventing malicious attacks. You can enable the BPDU source MAC address check in interface configuration mode for a specific port. One port can only filter one MAC address.	
Configuration Examples	The following example indicates only the BPDU with 00d0.f800.1e2f as the source MAC address will be received by interface Gi 1/1 . <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id-interface-id)# bpdu src-mac-check 00d0.f800.1e2f</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.2 bridge-frame forwarding protocol bpdu

	Use this command to enable BPDU transparent transmission. Use the no form of this command to restore the default setting.	
	bridge-frame forwarding protocol bpdu	
	no bridge-frame forwarding protocol bpdu	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	In the IEEE 802.1Q standard, 01-80-C2-00-00-00, the destination MAC address of BPDU frames, is reserved. Devices following the IEEE 802.1Q standard don't forward BPDU frames. In real network deployment, devices may be required to support BPDU transparent transmission. For example, when a device is not enabled with STP, BPDU transparent transmission can help implement STP calculation. BPDU transparent transmission works only when STP is disabled.	
Configuration Examples	The following example enables BPDU transparent transmission. <pre>FS(config)# bridge-frame forwarding protocol bpdu</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.3 clear spanning-tree counters

	Use this command to clear the statistics of the sent and received STP packets.	
	clear spanning-tree detected-protocols [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	ID of the interface
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	It is used to clear the statistics of the sent and received STP packets.	
Configuration Examples	The following example clears the statistics of the sent and received STP packets. <pre>FS# clear spanning-tree counters</pre>	

	The following example clears the statistics of the sent and received packets on interface Gi 0/1.	
	FS# clear spanning-tree counters interface gigabitethernet 0/1	
Related Commands	Command	Description
	show spanning-tree counters	Displays the statistics of STP transceived packets.
Platform Description	N/A	

7.4 clear spanning-tree detected-protocols

	Use this command to force the interface to send the RSTP BPDU message and check the BPDU messages.	
	clear spanning-tree detected-protocols [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	ID of the interface
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to force the interface to send the RSTP BPDU message.	
Configuration Examples	Forces to check the version of all interfaces.	
	FS# clear spanning-tree detected-protocols	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.5 clear spanning-tree mst topochange record

	Use this command to clear STP topology change record.
	clear spanning-tree mst <i>instance-id</i> topochange record

Parameter Description	Parameter	Description
	<i>instance-id</i>	Instance ID. For STP and RSTP protocols, only instance 0 is valid.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears STP topology change record. <pre>FS# show spanning-tree mst 0 topochange record Topology change information on mst 0: Time Interface Old status New status Type ----- 2013.5.1 4:18:46 Gi0/6 Learning Forwarding Normal FS# clear spanning-tree mst 0 topochange record FS# show spanning-tree mst 0 topochange record %There's no topology change information has been record on mst 0.</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.6 instance instance-id vlan vlan-range

	Use this command to set instance and VLAN mapping relations. Use the no form of the command to restore the default setting.	
	instance <i>instance-id</i> vlan <i>vlan-range</i>	
	no instance <i>instance-id</i> { vlan <i>vlan-range</i> }	
Parameter Description	Parameter	Description
	<i>instance-id</i>	Instance ID, in the range from 0 to 64
	<i>vlan-range</i>	VLAN range, in the range from 1 to 4094.
Defaults	The default is instance 0.	
Command Mode	MST configuration mode	

Usage Guide	instance <i>instance-id</i> vlan <i>vlan-range</i> : Add VLAN to MST instance. Instance-ID is in the range from 0 to 64 and VLAN is in the range from 1 to 4094. Use commas to separate VLAN IDs and use hyphen to indicate VLAN range, e.g., instance 10 vlan 2,3,6-9, which adds VLAN 2, 3, 4, 5, 6, 7, 8, 9 to instance 10. By default, all VLANs are in instance 0. Use the no form of this command to remove VLAN from instance 1-64. If you create 64 instances by stacking on a FS device with a small memory (e.g., 64M), the memory may be undersized. It is recommended to limit stacking instance number.	
Configuration Examples	This example enters MST mode and maps VLAN 3 and 5-10 to MST instance1. <pre>FS(config)# spanning-tree mst configuration FS(config-mst)# instance 1 vlan 3, 5-10 FS(config-mst)# show spanning-tree mst configuration Multi spanning tree protocol : Enable Name : Revision : 0 Instance Vlans Mapped ----- 0 1-2,4,11-4094 1 3,5-10 ----- FS(config-mst)# exit FS(config)#</pre> The following example removes VLAN3 from instance 1. <pre>FS(config-mst)# no instance 1 vlan 3</pre> The following example removes instance 1. <pre>FS(config-mst)# no instance 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 l2protocol-tunnel stp

	Use this command to enable BPDU TUNNEL globally. Use the no form of this command to disable this function.	
	l2protocol-tunnel stp	
	no l2protocol-tunnel stp	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.	
Configuration Examples	The following example enables BPDU TUNNEL globally. <pre>FS(config)# l2protocol-tunnel stp FS(config)# show l2protocol-tunnel stp L2protocol-tunnel: stp Enable L2protocol-tunnel destination mac address: 01d0.f800.0005</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.8 l2protocol-tunnel stp enable

	Use this command to enable BPDU TUNNEL on the interface. Use the no form of this command to disable this function.	
	l2protocol-tunnel stp enable	
	no l2protocol-tunnel stp enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	If you want to BPDU TUNNEL globally, enable BPDU TUNNEL on the interface first.	
Configuration Examples	The following example enables BPDU TUNNEL on the interface. <pre>FS(config-if-interface-id)# l2protocol-tunnel stp enable FS(config-if-interface-id)# show l2protocol-tunnel stp L2protocol-tunnel: stp Enable</pre>	

	L2protocol-tunnel destination mac address: 01d0.f800.0005 GigabitEthernet 0/1 l2protocol-tunnel stp enable	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.9 l2protocol-tunnel stp tunnel-dmac

	Use this command to configure the STP address for transparent transmission through BPDU TUNNEL. Use the no form of this command to restore the default setting.	
	l2protocol-tunnel stp tunnel-dmac <i>mac-address</i>	
	no l2protocol-tunnel stp tunnel-dmac	
Parameter Description	Parameter	Description
	<i>mac-address</i>	The STP address for transparent transmission.
Defaults		
Command Mode	Global configuration mode	
Usage Guide	The available STP address includes 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1, and 0100.0ccd.cdd2.	
Configuration Examples	The following example configures the STP address for transparent transmission through BPDU TUNNEL. FS(config)# l2protocol-tunnel stp tunnel-dmac 011a.a900.0005	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.10 name

	Use this command to set MST name. Use the no form of the command to restore the default setting.
	name <i>name</i>
	no name

Parameter Description	Parameter	Description
	<i>name</i>	MST name, up to 32 characters.
Defaults	The default is NULL.	
Command Mode	MST configuration mode	
Usage Guide	name <i>name</i> : Sets the MST name, up to 32 characters. show spanning-tree mst configuration : Displays MST region information.	
Configuration Examples	This example sets MST name to region1. <pre> FS(config)# spanning-tree mst configuration FS(config-mst)# name region1 FS(config-mst)# show spanning-tree mst configuration Multi spanning tree protocol : Enable Name : region1 Revision : 0 Instance Vlans Mapped ----- 0 : ALL FS(config-mst)# exit FS(config)# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.11 revision

	Use this command to set revision number of MSTP region. Use the no form of the command to restore the default setting.	
	revision <i>version</i>	
	no revision	
Parameter Description	Parameter	Description
	<i>version</i>	MST revision number, in the range from 0 to 65535.

Defaults	The default is 0.	
Command Mode	MST configuration mode	
Usage Guide	revision version: Sets the MST version, in the range from 0 to 65535. show spanning-tree mst configuration: Displays MST region information.	
Configuration Examples	This example sets revision number to 1. <pre> FS(config)# spanning-tree mst configuration FS(config-mst)# revision 1 FS(config-mst)# show spanning-tree mst configuration Multi spanning tree protocol : Enable Name : Revision : 1 Instance Vlans Mapped ----- 0 : ALL FS(config-mst)# exit FS(config)# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.12 show l2protocol-tunnel stp

	Use this command to display BPDU TUNNEL configuration.	
	show l2protocol-tunnel stp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode / Global configuration mode / Interface configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example displays BPDU TUNNEL configuration. <pre>FS# show l2protocol-tunnel stp L2protocol-tunnel: stp Enable L2protocol-tunnel destination mac address:011a.a900.0005 GigabitEthernet 0/1 l2protocol-tunnel stp enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.13 show spanning-tree

	Use this command to display the global spanning-tree configuration.	
	show spanning-tree [summary forward-time hello-time max-age inconsistentports tx-hold-count pathcost method max_hops counters]	
Parameter Description	Parameter	Description
	<i>summary</i>	Displays the information of MSTP instances and forwarding status of the interfaces.
	<i>inconsistentports</i>	Displays the block port due to root guard or loop guard.
	<i>forward-time</i>	Displays BridgeForwardDelay.
	<i>hello-time</i>	Displays BridgeHelloTime.
	<i>max-age</i>	Displays BridgeMaxAge.
	<i>max-hops</i>	Displays the maximum hops of an instance.
	<i>tx-hold-count</i>	Displays TxHoldCount.
	<i>pathcost method</i>	Displays the method used for calculating path cost.
	<i>counters</i>	Displays the statistics of STP transceived packets.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode and interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the global spanning-tree configuration. <pre>FS# show spanning-tree hello-time</pre>	

The following example displays the sent and received STP packets. <pre> FS# show spanning-tree counters ----- STP BPDU count ----- Port Receive Send GigabitEthernet 0/3 0 122594 ----- STP TC or TCN count ----- MSTID Port Receive Send 0 GigabitEthernet 0/3 0 0 </pre>		
Related Commands	Command	Description
	spanning-tree pathcost method	Sets the pathcost method.
	spanning-tree forward-time	Sets BridgeForwardDelay.
	spanning-tree hello-time	Sets BridgeHelloTime.
	spanning-tree max-age	Sets BridgeMaxAge.
	spanning-tree max-hops	Sets the maximum hops of an instance.
	spanning-tree tx-hold-count	Displays TxHoldCount.
Platform Description	N/A	

7.14 show spanning-tree interface

Use this command to display the STP configuration of the interface, including the optional spanning tree.		
show spanning-tree interface <i>interface-id</i> [{ bpdupfilter portfast bpduguard link-type }]		
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID
	bpdupfilter	Displays the status of BPDU filter.
	portfast	Displays the status of portfast.
	bpduguard	Displays the status of BPDU guard.
	link-type	Displays the link type of an interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode and interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the STP configuration on interface Gi 0/1. <pre> FS# show spanning-tree int gi 0/1 </pre>	

```

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : None

##### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost : 0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort

```

Related Commands	Command	Description
	spanning-tree bpdupfilter	Enables the BPDU filter feature someone the interface.
	spanning-tree portfast	Enables the portfast on the interface.
	spanning-tree bpduguard	Enables the BPDU guard on the interface.
	spanning-tree link-type	Sets the link type of the interface to point-to-point.
Platform Description	N/A	

7.15 show spanning-tree mst

	Use this command to display the information of MST and instances.	
	show spanning-tree mst { configuration instance-id [interface interface-id] }	
Parameter Description	Parameter	Description
	configuration	The MST configuration of the equipment.

	<i>instance-id</i>	Instance number
	<i>interface-id</i>	Interface number
Defaults	All the instances are displayed by default.	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information of MST and instances.	
	FS# show spanning-tree mst configuration	
	Multi spanning tree protocol : Enable	
	Name : test	
	Revision : 0	
	Instance Vlans Mapped	

	0 : 2-4094	
	1 : 1	
	Field Description	
	Field	Description
	Multi spanning tree protocol	Enables MSTP protocol.
	Name	Name of the MST region
	Revision	Revision of the MST region
	Instance Vlans Mapped	Mapping relation between the instance and VLAN
Related Commands	Command	Description
	spanning-tree mst configuration	Configures the MST region.
	spanning-tree mst cost	Displays the path cost of the instance.
	spanning-tree mst max-hops	Displays the maximum hops of the instance.
	spanning-tree mst priority	Displays the equipment priority of the instance.
	spanning-tree mst port-priority	Displays the port priority of the instance.
Platform Description	N/A	

7.16 show spanning-tree mst topochange record

	Use this command to display the STP topology change record.
	show spanning-tree mst <i>instance-id</i> topochange record

Parameter Description	Parameter	Description			
	<i>instance-id</i>	Instance ID.			
Defaults	N/A				
Command Mode	Privileged EXEC mode / Global configuration mode / Interface configuration mode				
Usage Guide	N/A				
Configuration Examples	The following example displays the STP topology change record of instance 0.				
	FS# show spanning-tree mst 0 topochange record				
	Topology change information on mst 0:				
	Time	Interface	Old status	New status	Type

	2013.5.1 4:18:46	Gi0/6	Learning	Forwarding	Normal
	Field	Description			
	Time	The time when the topology changes.			
	Interface	The interface whose topology changes.			
	Old status	Old STP status on the interface.			
New status	New STP status on the interface.				
Type	Topology change may be caused by the following causes: Normal: UP/DOWN state change on the interface, LoopGuard Block: Loop-inconsistence causes the interface to be blocked. RootGuard Block: Root-inconsistence causes the interface to be blocked. Inferior Block: Receiving inferior BPDU frames causes the interface to be blocked. LoopGuard Unblock: The interface returns to Forward status from loop-inconsistence. RootGuard Unblock: The interface returns to Forward status from root-inconsistence. Inferior Unblock-The interface returns to Forward status after not receiving inferior BPDU frames.				
Related Commands	Command		Description		
	N/A		N/A		
Platform Description	N/A				

7.17 spanning-tree

Use this command to enable MSTP and configure its basic settings globally. The **no** form of the command disables the spanning-tree function. The **no** form of the command with parameters only restores the corresponding parameters to the default values, but does not disable the spanning-tree function.

	spanning-tree [forward-time <i>seconds</i> hello-time <i>seconds</i> max-age <i>seconds</i>]	
	no spanning-tree [forward-time hello-time max-age]	
Parameter Description	Parameter	Description
	forward-time <i>seconds</i>	Interval at which the port status changes, in the range from 4 to 30 in the unit of seconds. The default is 15.
	hello-time <i>seconds</i>	Interval at which the switch sends the BPDU message, in the range from 1 to 10 in the unit of seconds. The default is 2.
	max-age <i>seconds</i>	Maximum aging time of the BPDU message, in the range from 6 to 40 in the unit of seconds. The default is 20.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	The values of forward-time, hello time and max-age are interrelated. Modifying one of these three parameters will affect the others. There is a restricted relationship among the above three values. $2 * (\text{Hello Time} + 1.0\text{snd}) \leq \text{Max-Age Time} \leq 2 * (\text{Forward-Delay} - 1.0\text{snd})$ If the values do not according with the condition, the settings do not work.	
Configuration Examples	The following example enables the spanning-tree function. <pre>FS(config)# spanning-tree</pre> The following example configures the BridgeForwardDelay. <pre>FS(config)# spanning-tree forward-time 10</pre>	
Related Commands	Command	Description
	show spanning-tree	Displays the global STP configuration.
	spanning-tree mst cost	Sets the PathCost of an STP interface.
	spanning-tree tx-hold-count	Sets the global TxHoldCount of STP.
Platform Description	N/A	

7.18 spanning-tree autoedge

	Use this command to enable Autoedge on the interface. Use the disabled form of this command to disable this function.
	spanning-tree autoedge [disabled]

Parameter Description	Parameter	Description
	disabled	Disabled Autoedge on the interface.
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3 seconds), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU. You can run the spanning-tree autoedge disabled command to disable Auto Edge.	
Configuration Examples	The following example disables Autoedge on the interface. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id-interface-id)# spanning-tree autoedge disabled</pre>	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration information of the interface.
Platform Description	N/A	

7.19 spanning-tree bpdupfilter

	Use this command to enable BPDU filter on the interface. You can use the enabled or disabled option of the command to enable or disable the BPDU filter function on the interface.	
	spanning-tree bpdupfilter [enabled disabled]	
Parameter Description	Parameter	Description
	enabled	Enables BPDU filter on the interface.
	disabled	Disables BPDU filter on the interface.
Defaults	This function is disabled by default,	
Command Mode	Interface configuration mode.	
Usage Guide	If BPDU filter is enabled on a port, the port neither sends nor receives BPDUs.	

Configuration	The following example enables BPDU filter on interface Gi 1/1.	
Examples	FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id-interface-id)# spanning-tree bpdupfilter enable	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.20 spanning-tree bpduguard

	Use this command to enable the BPDU guard function on the interface. You can use the enabled or disabled option of the command to enable or disable the BPDU guard function on the interface.	
	spanning-tree bpduguard [enabled disabled]	
Parameter Description	Parameter	Description
	enabled	Enables BPDU guard on the interface.
	disabled	Disables BPDU guard on the interface.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	1. If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU. 2. Run command errdisable recovery [interval seconds] to recover the interface in Error-disabled state.	
Configuration Examples	The following example enables the BPDU guard function on the interface. FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id-interface-id)# spanning-tree bpduguard enable	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.21 spanning-tree compatible enable

	Use this command to send the message selectively carried with MSTI according to the interface attribute of

	current port to realize interconnection with other vendors. Use the no form of this command to restore the default setting.	
	spanning-tree compatible enable	
	no spanning-tree compatible enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default. .	
Command Mode	Interface configuration mode.	
Usage Guide	If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the current port to realize interconnection between FS devices and other SPs' devices.	
Configuration Examples	The following example enables the compatibility mode on interface Gi 0/1. <pre>FS(config)# interface gigabitethernet 0/1 FS(config-if-interface-id-interface-id)#spanning-tree compatible enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.22 spanning-tree guard loop

	Use this command to enable loop guard on the interface to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the no form of this command to disable loop guard .	
	spanning-tree guard loop	
	no spanning-tree guard loop	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	

Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure. The loop guard function and root guard function cannot be enabled at the same time.	
Configuration Examples	The following example enables loop guard on interface Gi 0/1. <pre>FS(config)# interface gigabitethernet 0/1 FS(config-if-interface-id)# spanning-tree guard loop</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.23 spanning-tree guard none

	Use this command to disable guard on the interface. Use the no form of this command to enable this function	
	spanning-tree guard none	
	no spanning-tree guard none	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example disables guard on interface Gi 0/1. <pre>FS(config)# interface gigabitethernet 0/1 FS(config-if-interface-id)# spanning-tree guard none</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.24 spanning-tree guard root

	Use this command to enable root guard on the interface to prevent the change of current root bridge position because of error configuration and illegal packet attack. Use the no form of this command to restore the default setting.	
	spanning-tree guard root	
	no spanning-tree guard root	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If root guard is enabled, the current root bridge will not change due to incorrect configuration or illegal packet attacks. The loop guard function and root guard function cannot be enabled at the same time.	
Configuration Examples	The following example enables root guard on the interface. <pre>FS(config)# interface gigabitethernet 0/1 FS(config-if-interface-id)# spanning-tree guard root</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.25 spanning-tree ignore tc

	Use this command to enable the tc filtering on the interface. Use the no form of this command to restore the default setting. With tc filtering enabled, the TC packets received on the interface will not be processed.	
	spanning-tree ignore tc	
	no spanning-tree ignore tc	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Interface configuration mode.	
Usage Guide	If TC filter is enabled on a port, the port does not process received TC packets.	
Configuration Examples	The following example enables the tc filtering on the interface. <pre>FS(config)# interface gigabitethernet 0/1 FS(config-if-interface-id)# spanning-tree ignore tc</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.26 spanning-tree link-type

	Use this command to configure the link type of the interface. Use the no form of this command to restore the default setting.	
	spanning-tree link-type [point-to-point shared]	
	no spanning-tree link-type	
Parameter Description	Parameter	Description
	point-to-point	Sets the link type of the interface to point-to-point.
	shared	Forcibly sets the link type of the interface to shared.
Defaults	For a full-duplex interface, its link type is set to point-to-point link; for a half-duplex interface, its link type is set to shared.	
Command Mode	Interface configuration mode.	
Usage Guide	If the link type of a port is point-to-point connection, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.	
Configuration Examples	The following example configures the link type of the interface. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id)# spanning-tree link-type point-to-point</pre>	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.

Platform	N/A
Description	

7.27 spanning-tree loopguard default

	Use this command to enable loop guard globally to prevent the root port or backup port from generating loop since they cannot receive bpdu. Use the no form of this command to restore the default setting.	
	spanning-tree loopguard default	
	no spanning-tree loopguard default	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receipt failure.	
Configuration Examples	The following example enables loop guard globally to prevent the root port or backup port from generating loop since they cannot receive bpdu. FS(config)# spanning-tree loopguard default	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

7.28 spanning-tree max-hops

	Use this command to set the maximum number of hops(Max-hopsCount) of the BPDU message in the global configuration mode, the number of hops in a region that the BPDU message passes before being dropped. This parameter takes effect for all instances. Use the no form of this command to restore the default setting.	
	spanning-tree max-hops hop-count	
	no spanning-tree max-hops	
Parameter Description	Parameter	Description
	<i>hop-count</i>	Number of hops in a region that the BPDU message passes before being dropped. The range is 1 to 40 hops.

Defaults	The default is 20 hops.	
Command Mode	Global configuration mode.	
Usage Guide	In the region, the BPDU message sent by the root bridge includes a Hop Count field. When the BPDU message passes a device, the Hop Count is decreased by 1 until it reaches 0, which indicates the BPDU message times out. The device will drop the BPDU message whose Hop Count is 0. Changing the max-hops command affects all instances.	
Configuration Examples	This example sets the max-hops of the spanning tree to 10 for all instances. FS(config)# spanning-tree max-hops 10	
Related Commands	Command	Description
	show spanning-tree	Displays the MSTP information.
Platform Description	N/A	

7.29 spanning-tree mode

	Use this command to set the STP version. Use the no form of the command to restore the default setting.	
	spanning-tree mode [stp rstp mstp]	
	no spanning-tree mode	
Parameter Description	Parameter	Description
	stp	Spanning tree protocol(IEEE 802.1d)
	rstp	Rapid spanning tree protocol(IEEE 802.1w)
	mstp	Multiple spanning tree protocol(IEEE 802.1s)
Defaults	The default is mstp .	
Command Mode	Global configuration mode.	
Usage Guide	However, some vendors' devices do not work according to 802.1 protocol standards, possibly causing incompatibility. If other vendors' devices are incompatible with FS devices, run this command to switch the STP mode to a lower version.	
Configuration Examples	The following example sets the STP version.	
	FS(config)# spanning-tree mode stp	

Related Commands		
	Command	Description
	show spanning-tree	Displays the spanning-tree configuration.
Platform Description	N/A	

7.30 spanning-tree mst configuration

	Use this command to enter the MST configuration mode in the global configuration mode and configure the MSTP region. Use the no form of the command to restore the default setting.	
	spanning-tree mst configuration	
	no spanning-tree mst configuration	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults		
Command Mode	Global configuration mode.	
Usage Guide	To return to the privileged EXEC mode, enter end or Ctrl+C. To return to the global configuration mode, enter exit. After entering the MST configuration mode, you can configure MSTP Region parameters:	
Configuration Examples	This example enters the MST configuration mode. <pre> FS(config)# spanning-tree mst configuration FS(config-mst)# instance 1 vlan 3, 5-10 FS(config-mst)# name region 1 FS(config-mst)# revision 1 FS(config-mst)# show spanning-tree mst configuration Multi spanning tree protocol : Enable Name : region1 Revision : 1Instance Vlans Mapped ----- 0 1-2,4,11-4094 1 3,5-10 ----- FS(config-mst)# exit FS(config)# </pre>	
Related Commands		
	Command	Description
	show spanning-tree mst	Displays the MST region configuration.
	instance <i>instance-id</i> vlan <i>vlan-range</i>	Adds VLANs to the MST instance.

	name	Configures the name of MST.
	revision	Configures the version of MST.
Platform Description	N/A	

7.31 spanning-tree mst cost

	Use this command to set the path cost of an instance in the interface configuration mode. Use the no form of the command to restore the default setting.	
	spanning-tree [mst instance-id] cost cost	
	no spanning-tree [mst instance-id] cost	
Parameter Description	Parameter	Description
	instance-id	Instance ID in the range from 0 to 64.
	cost	Path cost in the range from 1 to 200,000,000.
Defaults	The default instance-id is 0. The default value is calculated by the link rate of the interface automatically. 1000 Mbps—20000 100 Mbps—200000 10 Mbps—2000000	
Command Mode	Interface configuration mode.	
Usage Guide	A higher cost value means a higher path cost.	
Configuration Examples	This example sets the path cost to 400 on the interface associated with instances 3. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if)# spanning-tree mst 3 cost 400</pre>	
Related Commands	Command	Description
	show spanning-tree mst	Displays the MSTP information of an interface.
	spanning-tree mst port-priority	Configures the priority of an interface.
	spanning-tree mst priority	Configures the priority of an instance.
Platform Description	N/A	

7.32 spanning-tree mst port-priority

	Use this command to configure the interface priority for different instances in the interface configuration mode. It will determine which interface of a loop in a region is in charge of forwarding. Use the no form of this command to restore the default setting.	
	spanning-tree [mst instance-id] port-priority priority	
	no spanning-tree [mst instance-id] port-priority	
Parameter Description	Parameter	Description
	Instance-id	Instance ID, in the range of 0 to 64
	priority	Interface priority. Sixteen integers are available: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, which are the multiples of 16.
Defaults	The default instance-id is 0. The default priority is 128.	
Command Mode	Interface configuration mode.	
Usage Guide	When a loop occurs in the region, the interface of the higher priority will be in charge of forwarding. If all interfaces have the same priority value, the interface of the smaller number will be in charge of the forwarding. Run this command to determine which port in the loop of a region enters the forwarding state.	
Configuration Examples	This example sets the priority of gigabitethernet 1/1 to 10 in instance 20. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id)# spanning-tree mst 20 port-priority 0</pre>	
Related Commands	Command	Description
	show spanning-tree mst	Displays the MSTP information of an interface.
	spanning-tree mst cost	Sets the path cost.
	spanning-tree mst priority	Sets the device priority for different instances.
Platform Description	N/A	

7.33 spanning-tree mst priority

	Use this command to set the device priority for different instances in the global configuration mode. Use the no form of this command to restore the default setting.	
	spanning-tree [mst instance-id] priority priority	
	no spanning-tree [mst instance-id] priority	

Parameter Description	Parameter	Description
	<i>instance-id</i>	Instance ID, in the range of 0 to 64
	<i>priority</i>	Device priority. Sixteen integers are available: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440, which are all multiples of 4096.
Defaults	The default instance ID is 0. The default device priority is 32768.	
Command Mode	Global configuration mode.	
Usage Guide	Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.	
Configuration Examples	The following example sets the device priority of the Instance to 8192. FS(config)# spanning-tree mst 20 priority 8192	
Related Commands	Command	Description
	show spanning-tree mst	Displays the MSTP information of an interface.
	spanning-tree mst cost	Sets path cost.
	spanning-tree mst port-priority	Sets the port priority of an instance.
Platform Description	N/A	

7.34 spanning-tree pathcost method

	Use this command to configure the path cost of the port. Use the no form of this command to restore the default setting.	
	spanning-tree pathcost method { { long [standard] short }	
	no spanning-tree pathcost method	
Parameter Description	Parameter	Description
	Long [standard]	Adopts the 802.1t standard to configure path cost. The standard indicates that use the expression recommended by the standard to calculate the cost value.
	short	Adopts the 802.1d standard to configure path cost.
Defaults	802.1T standard is adopted to set path cost by default.	

Command Mode	Global configuration mode.	
Usage Guide	If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.	
Configuration Examples	The following example configures the path cost of the port.	
	FS(config-if)# spanning-tree pathcost method long	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.35 spanning-tree portfast

	Use this command to enable the portfast on the interface. Use the disabled form of this command to restore the default setting,	
	spanning-tree portfast [disabled]	
Parameter Description	Parameter	Description
	disabled	Disables the portfast on the interface.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	After PortFast is enabled on a port, the port directly enters the forwarding state. However, since the Port Fast Operational State becomes disabled due to receipt of BPDUs, the port can properly run the STP algorithm and enter the forwarding state.	
Configuration Examples	The following example enables the portfast on the interface. FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id)# spanning-tree portfast	
Related Commands	Command	Description
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.36 spanning-tree portfast bpdudfilter default

	Use this command to enable the BPDU filter function globally. You can use the no form of the command to restore the default setting.	
	spanning-tree portfast bpdudfilter default	
	no spanning-tree portfast bpdudfilter default	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default,	
Command Mode	Global configuration mode.	
Usage Guide	Once the BPDU filter is enabled, the BPDU message is neither received nor sent on the interface. Use the show spanning-tree command to display the configuration.	
Configuration Examples	The following example enables the BPDU filter function globally.	
	FS(config)# spanning-tree portfast bpdudfilter default	
Related Commands	Command	Description
	show spanning-tree interface	Displays the global STP configuration.
Platform Description	N/A	

7.37 spanning-tree portfast bpduguard default

	Use this command to enable the BPDU guard globally. Use the no form of this command to restore the default setting,	
	spanning-tree portfast bpduguard default	
	no spanning-tree portfast bpduguard default	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	

Usage Guide	Once the BPDU guard is enabled on the interface, it will enter the error-disabled status if the BPDU message arrives at the interface. Use the show spanning-tree command to display the configuration.	
	 The global BPDU guard takes effect only when PortFast is enabled on a port.	
Configuration Examples	The following example enables the BPDU guard globally. <pre>FS(config)# spanning-tree portfast bpduguard default</pre>	
Related Commands	Command	Description
	show spanning-tree interface	Displays the global STP configuration.
Platform Description	N/A	

7.38 spanning-tree portfast default

	Use this command to enable the portfast feature on all interfaces globally. Use the no form of this command to restore the default setting.	
	spanning-tree portfast default	
	no spanning-tree portfast default	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example enables the portfast feature on all interfaces globally. <pre>FS(config)# spanning-tree portfast default</pre>	
Related Commands	Command	Description
	show spanning-tree interface	Displays the global STP configuration.
Platform Description	N/A	

7.39 spanning-tree reset

	Use this command to restore the spanning-tree configuration to the default setting.	
	spanning-tree reset	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	Enable TC guard to prevent TC packets from spreading.	
Configuration Examples	The following example enables tc-guard on interface Gi 1/1. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if-interface-id)# spanning-tree tc-guard</pre>	
Related Commands	Command	Description
	show spanning-tree	Displays the global STP configuration.
	show spanning-tree interface	Displays the STP configuration of the interface.
Platform Description	N/A	

7.40 spanning-tree tc-guard

	Use this command to enable tc-guard on the interface to prevent the spread of TC messages. Use the no form of this command to disable this function on the interface.	
	spanning-tree tc-guard	
	no spanning-tree tc-guard	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	

Usage Guide	N/A	
Configuration Examples	The following example enables tc-guard on the interface to prevent the spread of TC messages. FS(config)# spanning-tree tc-guard	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.41 spanning-tree tc-protection

	Use this command to enable tc-protection globally. Use The no form of this command to disable this function.	
	spanning-tree tc- protection	
	no spanning-tree tc- protection	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example enables tc-protection globally. FS(config)# spanning-tree tc-protection	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.42 spanning-tree tc-protection tc-guard

	Use this command to enable tc-guard to prevent TC packets from being flooded. Use the no form of this command to restore the default setting.	
	spanning-tree tc-protection tc-guard	
	no spanning-tree tc-protection tc-guard	
Parameter	Parameter	Description

Description		
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	Enable TC guard to prevent TC packets from spreading.	
Configuration Examples	The following example enables tc-guard to prevent TC packets from being flooded. FS(config)# spanning-tree tc-protection tc-guard	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.43 spanning-tree tx-hold-count

	Use this command to configure the TxHoldCount of the STP, the maximum number of the BPDU messages sent in one second. Use the no form of this command to restore the default setting.	
	spanning-tree tx-hold-count tx-hold-count no spanning-tree tx-hold-count	
Parameter Description	Parameter	Description
	tx-hold-count	Indicates the maximum number of BPDUs sent per second. The value ranges from 1 to 10. The default value is 3.
Defaults	The default is 3.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the maximum number of the BPDU messages sent in one second. FS(config)# spanning-tree tx-hold-count 5	
Related Commands	Command	Description
	show spanning-tree	Displays the global MSTP configuration.
Platform Description	N/A	

8 GVRP Commands

8.1 bridge-frame forwarding protocol gvrp

	Use this command to enable GVRP PDUs transparent transmission. Use the no form of this command to restore the default setting.	
	bridge-frame forwarding protocol gvrp	
	no bridge-frame forwarding protocol gvrp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	In the IEEE 802.1Q standard, the MAC address 01-80-C2-00-00-21 of GVRP PDUs is reserved for future standardization. In other words, the device following the IEEE 802.1Q standard does not forward GVRP PDUs frames. However, in actual network deployment, GVRP PDUs transparent transmission may be required. For example, the device not enabled with GVRP needs to transmit GVRP PDUs frames transparently to ensure proper GVRP topology calculation.	
Configuration Examples	The following example enables GVRP PDUs transparent transmission. FS(config)# bridge-frame forwarding protocol gvrp	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.2 clear gvrp statistic

	Use this command to clear the GVRP statistics for re-counting.	
	clear gvrp statistics { interface-id all }	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface id
Defaults	N/A	

Command mode	Privileged EXEC mode.	
Usage Guide	Use the show gvrp statistics to display the statistics.	
Configuration Examples	The following example clears GVRP statistics. <pre>FS# clear gvrp statistics all</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.3 gvrp applicant state

	Use this command configures the GVRP advertisement mode on the interface.. Use the no form of this command to restore default setting.	
	gvrp applicant state { normal non-applicant }	
	no gvrp applicant state	
Parameter Description	Parameter	Description
	normal	The interface sends VLAN advertisement.
	non-applicant	The interface does not send VLAN advertisement.
Defaults	The interface sends GVRP advertisement by default.	
Command mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the GVRP advertisement mode on the interface. <pre>FS(config-if)# gvrp applicant state normal</pre>	
Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configurations.
Platform	N/A	

Description	

8.4 gvrp dynamic-vlan-creation

	Use this command to enable dynamic VLAN creation. Use the no form of this command to restore the default setting.	
	gvrp dynamic-vlan-creation enable	
	no gvrp dynamic-vlan-creation enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	Use the show gvrp configuration to display the configuration.	
Configuration Examples	The following example enables dynamic VLAN creation. FS(config)# gvrp dynamic-vlan-creation enable	
Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configurations.
Platform Description	N/A	

8.5 gvrp enable

	Use this command to enable the GVRP function. Use the no form of this command to restore the default setting.	
	gvrp enable	
	no gvrp enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Global configuration mode	

Usage Guide	This command is used to display the configuration.	
Configuration Examples	The following example enables the GVRP function. FS(config)#gvrp enable	
Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configurations.
Platform Description	N/A	

8.6 gvrp registration mode

	Use this command to set the registration mode to control whether to enable dynamic VLAN creation/registration/canceling on the port. Use the no form of this command to restore the default setting.	
	gvrp registration mode { normal disabled }	
	no gvrp registration mode	
Parameter Description	Parameter	Description
	normal	Enables dynamic VLAN creation/registration/canceling on the port.
	disabled	Disables dynamic VLAN creation/registration/canceling on the port.
Defaults	Dynamic VLAN creation/registration/canceling is enabled by default,	
Command mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the registration mode. FS(config-if)# gvrp registration mode normal	
Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configurations.
Platform Description	N/A	

8.7 gvrp timer

	Use this command to set the GVRP timer. Use the no form of this command to restore the default setting.	
	gvrp timer { join <i>timer_value</i> leave <i>timer_value</i> leaveall <i>timer_value</i> }	
	no gvrp timer	
Parameter Description	Parameter	Description
	<i>join timer_value</i>	Controls the maximum delay before sending the advertisement on the port. The actual sending interval is in the range of 0 to the maximum delay.
	<i>leave timer_value</i>	Controls the waiting time before removing the VLAN from the port with the Leave Message received. If the Join Message is received again within this time range, the port-VLAN relation still exists and the timer becomes invalid. If no Join Message is received on the port, the port status will be the Empty and removed from the VLAN member list.
	<i>leave all timer_value</i>	Controls the minimum interval of sending the LeaveAll Message on the port. If the LeaveAll Message is received before the timer expires, the timer re-counts. If the timer expires, send the LeaveAll Message on the port and also send this Message to the port, so that the Leave timer begins counting. The actual sending interval ranges from leaveall to leaveall+join.
Defaults	Join timer: 200 milliseconds; Leave timer: 600 milliseconds; Leaveall timer: 10000 milliseconds.	
Command mode	Global configuration mode	
Usage Guide	Use the show gvrp configuration to display the configuration. Use the no gvrp timer command to restore join , leave and leaveall timer to default settings.	
Configuration Examples	The following example configures the join timer. FS(config)# gvrp timer join 200	
Related Commands	Command	Description
	show gvrp configuration	Displays the GVRP configuration.
Platform Description	N/A	

8.8 l2protocol-tunnel gvrp

	Use this command to enable global GVRP PDUs TUNNEL globally. Use the no form of this command to restore the default setting.	
	l2protocol-tunnel gvrp	
	no l2protocol-tunnel gvrp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.	
Configuration Examples	The following example enables GVRP PDUs TUNNEL globally. <pre>FS(config)# l2protocol-tunnel gvrp FS(config)# show l2protocol-tunnel gvrp L2protocol-tunnel: Gvrp Disable L2protocol-tunnel destination mac address:01d0.f800.0006</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.9 l2protocol-tunnel gvrp enable

	Use this command to enable GVRP PDUs TUNNEL on the interface. Use this command to restore the default setting.	
	l2protocol-tunnel gvrp enable	
	no l2protocol-tunnel gvrp enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command mode	Interface configuration mode	
Usage Guide	If you want to enable global GVRP PDUs TUNNEL, enable GVRP PDUs TUNNEL on the interface first.	
Configuration Examples	The following example enables GVRP PDUs TUNNEL on the interface. <pre>FS(config-if-interface-id)# l2protocol-tunnel gvrp enable FS(config-if-interface-id)# show l2protocol-tunnel gvrp</pre> L2protocol-tunnel: Gvrp Disable L2protocol-tunnel destination mac address:01d0.f800.0006 GigabitEthernet 0/1 l2protocol-tunnel gvrp enable	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.10 l2protocol-tunnel gvrp tunnel-dmac

	Use this command to configure the MAC address for transparent transmission in GVRP PDUs TUNNEL. Use the no form of this command to restore the default setting.	
	l2protocol-tunnel gvrp tunnel-dmac <i>mac-address</i>	
	no l2protocol-tunnel gvrp tunnel-dmac	
Parameter Description	Parameter	Description
	<i>mac-address</i>	The MAC address for transparent transmission in GVRP PDUs TUNNEL.
Defaults	The default is 01d0.f800.0006.	
Command mode	Global configuration mode	
Usage Guide	The available MAC address f ranges from 01d0.f800.0006 to 011a.a900.0006.	
Configuration Examples	The following example configures the MAC address for transparent transmission in GVRP PDUs TUNNEL. <pre>FS(config)# l2protocol-tunnel gvrp tunnel-dmac 011a.a900.0006</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.11 show gvrp configuration

	Use this command to display the GVRP configuration.																									
	show gvrp configuration																									
Parameter Description	Parameter	Description																								
	N/A	N/A																								
Defaults	N/A																									
Command mode	Privileged EXEC mode.																									
Usage Guide	Use the show gvrp configuration to display the configuration.																									
Configuration Examples	The following example displays GVRP configuration. Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: <table><thead><tr><th>PORT</th><th>Applicant Status</th><th>Registration Mode</th></tr></thead><tbody><tr><td>GigabitEthernet 0/2</td><td>normal</td><td>normal</td></tr></tbody></table> <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>GVRP Feature</td><td>Whether to enable GVRP</td></tr><tr><td>GVRP dynamic VLAN creation</td><td>Whether to enable dynamic VLAN creation</td></tr><tr><td>Join Timers</td><td>Join timer</td></tr><tr><td>Leave Timers</td><td>Leave timer</td></tr><tr><td>Leaveall Timers</td><td>Leaveall timer</td></tr><tr><td>PORT</td><td>Port</td></tr><tr><td>Applicant Status</td><td>Advertisement mode</td></tr><tr><td>Registration Mode</td><td>Registration mode</td></tr></tbody></table>		PORT	Applicant Status	Registration Mode	GigabitEthernet 0/2	normal	normal	Field	Description	GVRP Feature	Whether to enable GVRP	GVRP dynamic VLAN creation	Whether to enable dynamic VLAN creation	Join Timers	Join timer	Leave Timers	Leave timer	Leaveall Timers	Leaveall timer	PORT	Port	Applicant Status	Advertisement mode	Registration Mode	Registration mode
PORT	Applicant Status	Registration Mode																								
GigabitEthernet 0/2	normal	normal																								
Field	Description																									
GVRP Feature	Whether to enable GVRP																									
GVRP dynamic VLAN creation	Whether to enable dynamic VLAN creation																									
Join Timers	Join timer																									
Leave Timers	Leave timer																									
Leaveall Timers	Leaveall timer																									
PORT	Port																									
Applicant Status	Advertisement mode																									
Registration Mode	Registration mode																									

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.12 show gvrp statistics

	Use this command to display the GVRP statistics of one interface or all interfaces.	
	show gvrp statistics { <i>interface-id</i> all }	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface id.
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	Use the show gvrp statistics to display the statistics of one interface or all interfaces.	
Configuration Examples	<pre> FS# show gvrp statistics gigabitethernet 1/1 Interface GigabitEthernet 3/1 RecValidGvrpPdu 0 RecInvalidGvrpPdu 0 RecJoinEmpty 0 RecJoinIn 0 RecEmpty 0 RecLeaveEmpty 0 RecLeaveIn 0 RecLeaveAll 0 SentGvrpPdu 0 SentJoinEmpty 0 SentJoinIn 0 SentEmpty 0 SentLeaveEmpty 0 SentLeaveIn 0 SentLeaveAll 0 JoinIndicated 0 LeaveIndicated 0 JoinPropagated 0 LeavePropagated 0 </pre>	

	Field	Description
	RecValidGvrpPdu	Number of received valid GPDUs packets.
	RecInvalidGvrpPdu	Number of received invalid GPDUs packets.
	RecJoinEmpty/ SentJoinEmpty	Number of received/sent JoinEmpty messages.
	RecJoinIn/ SentJoinIn	Number of received/sent JoinIn messages.
	RecEmpty/SentEmpty	Number of received/sent Empty messages.
	RecLeaveEmpty/SentLeaveEmpty	Number of received/sent LeaveEmpty messages.
	RecLeaveIn/ SentLeaveIn	Number of received/sent LeaveIn messages.
	RecLeaveAll/SentLeaveAll	Number of received/sent LeaveAll messages.
	SentGvrpPdu	Number of sent GPDUs messages.
	JoinIndicated/ LeaveIndicated	Number of Join/Leave service requests.
	JoinPropagated / LeavePropagated	Number of Join/Leave topology update requests.
Related Commands	Command	Description
	clear gvrp statistics	Clears the statistics of one interface or all interfaces.
Platform Description	N/A	

8.13 show gvrp status

	Use this command to display all dynamic VLAN ports generated by GVRP and the dynamic VLAN ports added to the static VLAN.	
	show gvrp status	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode.	
Usage Guide	Use the show gvrp status command to display the GVRP status.	
Configuration Examples	The following example displays the GVRP status. <pre> FS# show gvrp status VLAN 1 Dynamic Ports: DVLAN 2 Dynamic Ports: </pre>	

	Field	Description
	VLAN	Static VLAN
	DVLAN	Dynamic VLAN
	Dynamic Ports	Dynamic ports.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.14 show l2protocol-tunnel gvrp

	Use this command to display GVRP PDUs TUNNEL configuration.	
	show l2protocol-tunnel gvrp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays GVRP PDUs TUNNEL configuration. FS# show l2protocol-tunnel gvrp L2protocol-tunnel: Gvrp Enable L2protocol-tunnel destination mac address:011a.a900.0006 GigabitEthernet 0/1 l2protocol-tunnel gvrp enable	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9 LLDP Commands

9.1 civic-location

	Use this command to configure a common LLDP address. Use the no form of this command to delete the address.	
	{ country state county city division neighborhood street-group leading-street-dir trailing-street-suffix street-suffix number street-number-suffix landmark additional-location-information name postal-code building unit floor room type-of-place postal-community-name post-office-box additional-code } <i>ca-word</i>	
	no { country state county city division neighborhood street-group leading-street-dir trailing-street-suffix street-suffix number street-number-suffix landmark additional-location-information name postal-code building unit floor room type-of-place postal-community-name post-office-box additional-code } <i>ca-word</i>	
Parameter	Parameter	Description
Description	country	Country code, two bytes. For example, the country code of China is CH.
	state	Address information, CA type 1
	county	CA type 2
	city	CA type 3
	division	CA type 4
	neighborhood	CA type 5
	street-group	CA type 6
	leading-street-dir	CA type 16
	trailing-street-suffix	CA type 17
	street-suffix	CA type 18
	number	CA type 19
	street-number-suffix	CA type 20
	landmark	CA type 21
	additional-location-information	CA type 22
	name	CA type 23
	postal-code	CA type 24
	building	CA type 25
	unit	CA type 26
	floor	CA type 27
	room	CA type 28
	type-of-place	CA type 29
	postal-community-name	CA type 30
	post-office-box	CA type 31
	additional-code	CA type 32
	<i>ca-word</i>	Address information
Defaults	N/A	

Command Mode	LLDP Civic address configuration mode	
Usage Guide	This command is used to configure a common LLDP address in LLDP Civic address configuration mode.	
Configuration Examples	The following example configures an LLDP Civic Address (ID: 1). <pre> FS#config FS(config)# lldp location civic-location identifier 1 FS(config-lldp-civic)# country CH FS(config-lldp-civic)# city Fuzhou </pre>	
Related Commands	Command	Description
	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays the information about an LLDP Civic address.
Platform Description	N/A	

9.2 clear lldp statistics

	Use this command to clear LLDP statistics.	
	clear lldp statistics [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	interface parameter: clear the LLDP statistics of the specified interface	
Configuration Examples	The following example clears LLDP statistics of interface 1. <pre> FS# clear lldp statistics interface GigabitEthernet 0/1 FS# show lldp statistics interface GigabitEthernet 0/1 Lldp statistics information of port [GigabitEthernet 0/1] ----- The number of lldp frames transmitted : 0 The number of frames discarded : 0 The number of error frames : 0 The number of lldp frames received : 0 The number of TLVs discarded : 0 </pre>	

	The number of TLVs unrecognized : 0 The number of neighbor information aged out : 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.3 clear lldp table

	Use this command to clear LLDP neighbor information.	
	clear lldp table [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If the interface parameter is specified, the LLDP neighbor information on the specified interface is cleared. If the interface parameter is not specified, the LLDP neighbor information on all interfaces is cleared.	
Configuration Examples	The following example clears the LLDP neighbor information on interface 1. <pre> FS# show lldp neighbors interface GigabitEthernet 0/1 Lldp statistics information of port [GigabitEthernet 0/1] ----- The number of lldp frames transmitted : 0 The number of frames discarded : 0 The number of error frames : 0 The number of lldp frames received : 0 The number of TLVs discarded : 0 The number of TLVs unrecognized : 0 The number of neighbor information aged out : 0 FS# clear lldp table interface GigabitEthernet 0/1 FS# show lldp neighbors interface GigabitEthernet 0/1 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.4 device-type

	Use this command to configure the device type. Use the no form of this command to restore the default setting.	
	device-type <i>device-type</i>	
	no device-type	
Parameter Description	Parameter	Description
	<i>device-type</i>	Device type. The value ranges from 0 to 2. 0: The device type is DHCP Server. 1: The device type is switch. 2: The device type is LLDP MED terminal.
Defaults		
Command Mode	LLDP Civic address configuration mode	
Usage Guide	This command is used to configure the device type in a common LLDP address in LLDP Civic address configuration mode.	
Configuration Examples	The following example sets the device type to switch. <pre>FS#config FS(config)# lldp location civic-location identifier 1 FS(config-lldp-civic)# device-type 1</pre>	
Related Commands	Command	Description
	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays LLDP Civic Address information.
Platform Description	N/A	

9.5 lldp enable

	Use this command to enable the LLDP globally or on the interface. Use no form of this command to disable this function.	
	lldp enable	
	no lldp enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	

Command Mode	Global (or interface) configuration mode					
Usage Guide	LLDP takes effect on an interface only when LLDP is enabled globally.					
Configuration Examples	The following example disables LLDP globally and on the interface. FS#config FS(config)#no lldp enable FS(config)#interface gigabitethernet 0/1 FS(config-if)# no lldp enable					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show lldp status</td><td>Displays LLDP status information.</td></tr></table>	Command	Description	show lldp status	Displays LLDP status information.	
Command	Description					
show lldp status	Displays LLDP status information.					
Platform Description	N/A					

9.6 lldp encapsulation snap

	Use this command to configure the encapsulation format of LLDP packets. Use the no form of this command to restore the default setting.	
	lldp encapsulation snap	
	no lldp encapsulation snap	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	By default, Ethernet II encapsulation format is used.	
Command Mode	Interface configuration mode.	
Usage Guide	 To guarantee the normal communication between local device and neighbor device, the same LLDP packet encapsulation format must be used.	
Configuration Examples	The following example sets LLDP packet encapsulation format to SNAP. FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if)#lldp encapsulation snap	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform	N/A
Description	

9.7 lldp error-detect

	Use this command to configure the LLDP error detection, including the detection of VLAN configurations on both sides of the link, port state detection, port aggregation configuration detection, MTU configuration detection and loop detection. If any error is detected by LLDP, warning message will be printed to notify the administrator. Use the no form of this command to disable this function.	
	lldp error-detect	
	no lldp error-detect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	LLDP error detection relies on the specific TLV in the LLDP packets exchanged between devices on both sides of the link. To ensure normal functioning of the detection feature, correct TLVs must be advertised.	
Configuration Examples	The following example configures LLDP error detection. <pre>FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if)#lldp error-detect</pre>	
Related Commands	Command	Description
	show interface status	Displays LLDP status information.
Platform	N/A	
Description		

9.8 lldp fast-count

	When a new neighbor is detected or when LLDP operating mode changes from shutdown or Rx to TxRx or Tx, to allow the neighbor device to quickly study the information about this device, the fast sending mechanism will be initiated. The fast sending mechanism shortens the LLDPDU sending interval to 1 second and continuously transmits a certain number of LLDPDUs before restoring to the normal transmit interval. Use the no form of this command to restore the default setting.	
	lldp fast-count value	
	no lldp fast-count	

Parameter	Parameter	Description
Description	value	The number of fast sent LLDP packets, in the range from 1 to 10.
Defaults	The default is 3.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the number of fast sent LLDP packets to 5. FS#config FS(config)#lldp fast-count 5	
Related Commands	Command	Description
	show interface status	Displays LLDP status information.
Platform Description	N/A	

9.9 lldp hold-multiplier

	Use this command to set the TTL multiplier. Use the no form of this command to restore to default setting.	
	lldp hold-multiplier <i>value</i>	
	no lldp hold-multiplier	
Parameter	Parameter	Description
Description	<i>value</i>	TTL multiplier, in the range from 2 to 10.
Defaults	The default is 4.	
Command Mode	Global configuration mode.	
Usage Guide	The value of Time To Live (TLV) in LLDP packet = TTL multiplier × LLDP packet transmit interval + 1. Therefore, the TTL of local device information on the neighbor device can be controlled by adjusting TTL multiplier.	
Configuration Examples	The following example sets TTL multiplier to 5. FS#config FS(config)#lldp hold-multiplier 5	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.

Platform	N/A
Description	

9.10 lldp ignore pvid-error-detect

	Use this command to enable the function of ignoring PVID function. Use the no form of this command to disable the function of ignoring PVID function.	
	lldp ignore pvid-error-detect	
	no lldp ignore pvid-error-detect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	By default, it is disabled.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example ignores PVID detection globally. <pre>FS# configure terminal FS(config)# lldp ignore pvid-error-detect</pre>	
Platform	N/A	
Description		

9.11 lldp location civic-location identifier

	Use this command to create a common address of a device connected to the network in LLDP Civic Address configuration mode. Use the no form of this command to delete the address.	
	lldp location civic-location identifier <i>id</i>	
	no lldp location civic-location identifier <i>id</i>	
Parameter	Parameter	Description
Description	<i>id</i>	ID of a common address of a network device, in the range from 1 to 1024.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command can be used to enter the LLDP Civic Address configuration mode.	

Configuration	The following example creates the Civic Address information in LLDP MED-TLV as follows: set <i>id</i> to 1.	
Examples	FS#config FS(config)#lldp location civic-location identifier 1 FS(config-lldp-civic)#	
Related	Command	Description
Commands	show lldp location civic-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays the LLDP Civic Address information.
Platform	N/A	
Description		

9.12 lldp location elin identifier

	Use this command to set an emergency number encapsulated in a Location Identification TLV. Use the no form of this command to delete the number.	
	lldp location elin identifier <i>id</i> elin-location <i>tel-number</i>	
	no lldp location elin identifier <i>id</i>	
Parameter	Parameter	Description
Description	<i>id</i>	ID of an emergency number, in the range from 1 to 1024.
	<i>tel-number</i>	Emergency number, in the range from 10 to 25 bytes.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure an emergency number.	
Configuration Examples	The following example sets an emergency number. FS#config FS(config)#lldp location elin identifier 1 elin-location 085283671111	
Related Commands	Command	Description
	show lldp location elin-location { identifier <i>id</i> interface <i>interface-name</i> static }	Displays an LLDP emergency number.
Platform Description	N/A	

9.13 lldp management-address-tlv

	Use this command to configure the management address advertised in LLDP packets. Use the no form of this command to disable the advertisement of management address.	
	lldp management-address-tlv [<i>ip-address</i>]	
	no lldp management-address-tlv	
Parameter	Parameter	Description
Description	<i>ip-address</i>	The management address advertised in LLDP packets.
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	By default, the management address is advertised in LLDP packets, and is the IPv4 address of the lowest-ID VLAN carried on the port. If IPv4 address is not configured for this VLAN, the next lowest-ID VLAN carried on the port will be tried until the IPv4 address is obtained. If the IPv4 address is still not found, the IPv6 address of the lowest-ID VLAN carried on the port will be tried. If the IPv6 address is still not found, the MAC address of the device will be advertised as the management address.	
Configuration Examples	The following example configures the management address advertised in LLDP packets to 192.168.1.1. <pre>FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if)#lldp management-address-tlv 192.168.1.1</pre>	
Related Commands	Command	Description
	show lldp local-information	Displays LLDP local information
Platform Description	N/A	

9.14 lldp mode

	Use this command to configure the LLDP operating mode. Use no form of this command to restore the default setting.	
	lldp mode { <i>rx</i> <i>tx</i> <i>txrx</i> }	
	no lldp mode	
Parameter	Parameter	Description
Description	rx	Only sends LLDPDUs.
	tx	Only receives LLDPDUs.
	txrx	Sends and receives LLDPDUs.

Defaults	The default is txrx .	
Command Mode	Interface configuration mode	
Usage Guide	Disable LLDP operating mode on the interface. The interface won't send and receive LLDP packets. The precondition for enabling LLDP on the interface is that LLDP has been enabled globally and LLDP operates in tx, rx or txrx mode.	
Configuration Examples	The following example sets LLDP operating mode to tx on the interface. FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if)#lldp mode tx	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information
Platform Description	N/A	

9.15 lldp network-policy profile

	Use this command to create an LLDP network policy and enter the LLDP network policy configuration mode. Use the no form of this command to delete the policy.	
	lldp network-policy profile <i>profile-num</i>	
	no lldp network-policy profile <i>profile-num</i>	
Parameter	Parameter	Description
Description	profile-num	ID of an LLDP network policy, in the range from 1 to 1024.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enter the LLDP network policy configuration mode. When this command is run, the policy ID must be specified. In LLDP network-policy mode, the { voice voice-signaling } vlan command can be used to configure the specific network policy.	
Configuration Examples	The following example creates an LLDP network policy whose ID is 1. <pre>FS#config</pre>	

	FS(config)#lldp network-policy profile 1 FS(config-lldp-network-policy)#	
Related Commands	Command	Description
	show lldp network-policy profile [<i>profile-num</i>]	Displays an LLDP network policy.
Platform Description	N/A	

9.16 lldp notification remote-change enable

	Use this command to configure LLDP Trap. Use the no form of this command to restore the default setting.	
	lldp notification remote-change enable	
	no lldp notification remote-change enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	By configuring LLDP Trap, the LLDP information of local device (such as information about the detection of new neighbor or the fault on the communication link) can be sent to the network management server. The administrator can monitor the network operation status according to such information.	
Configuration Examples	The following example configures LLDP Trap. <pre> FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if)#lldp notification remote-change enable </pre>	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.
Platform Description	N/A	

9.17 lldp timer notification-interval

	Use this command to set an interval of sending LLDP Traps. Use the no form of this command to restore the default setting.
	lldp timer notification-interval <i>seconds</i>

	no lldp timer notification-interval	
Parameter	Parameter	Description
Description	<i>seconds</i>	Interval of sending LLDP Traps, in the range from 5 to 3600 in the unit of seconds.
Defaults	The default is 5.	
Command Mode	Global configuration mode.	
Usage Guide	To prevent excessive LLDP traps from being sent, you can set an interval of sending LLDP Traps. If LLDP information change is detected during this interval, traps will be sent to the network management server.	
Configuration Examples	The following example sets the interval of sending LLDP Traps to 10 seconds. <pre>FS#config FS(config)#lldp timer notification-interval 10</pre>	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.
Platform	N/A	
Description		

9.18 lldp timer reinit-delay

	Use this command to set port initialization delay. Use the no form of this command to restore the default setting.	
	lldp timer reinit-delay <i>seconds</i>	
	no lldp timer reinit-delay	
Parameter	Parameter	Description
Description	<i>seconds</i>	Port initialization delay, in the range from 1 to 10 in the unit of seconds.
Defaults	The default is 2.	
Command Mode	Global configuration mode.	
Usage Guide	To prevent LLDP from being initialized too frequently due to the frequent operating mode change, you can configure port initialization delay.	
Configuration	The following example sets LLDP port initialization delay to 3 seconds.	

Examples	FS#config	
	FS(config)#lldp timer reinit-delay 3	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.
Platform Description	N/A	

9.19 lldp timer tx-delay

	Use this command to set LLDP packet transmission delay. Use the no form of this command to restore the default setting.	
	lldp timer tx-delay <i>seconds</i>	
	no lldp timer tx-delay	
Parameter Description	Parameter	Description
	<i>seconds</i>	LLDP packet transmission delay, in the range from 1 to 8192 in the unit of seconds.
Defaults	The default is 2.	
Command Mode	Global configuration mode.	
Usage Guide	An LLDP-enabled port will send LLDP packets when the local device information changes. To avoid frequently sending LLDP packets due to the frequent local device information change, configure the LLDP packet transmission delay to control the frequent transmission of LLDP packets.	
Configuration Examples	The following example sets LLDPDU transmission delay to 3 seconds.	
	FS#config FS(config)#lldp timer tx-delay 3	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.
Platform Description	N/A	

9.20 lldp timer tx-interval

	Use this command to set the interval of sending the LLDP packets. Use no form of this command to restore the default setting.	
	lldp timer tx-interval <i>seconds</i>	
	no lldp timer tx-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval of sending the LLDP packets, in the range from 5 to 32768 in the unit of seconds.
Defaults	The default is 30.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the interval of sending the LLDP packets to 10 seconds.	
	<pre>FS#config FS(config)#lldp timer tx-interval 10</pre>	
Related Commands	Command	Description
	show lldp status	Displays LLDP status information.
Platform Description	N/A	

9.21 lldp tlv-enable

	Use this command to configure the types of advertisable TLVs. Use the no form of this command to restore the default setting.	
	<pre>lldp tlv-enable { basic-tlv { all port-description system-capability system-description system-name } dot1-tlv { all port-vlan-id protocol-vlan-id [vlan-id] vlan-name [vlan-id] } dot3-tlv { all link-aggregation mac-physic max-frame-size power } med-tlv { all capability inventory location { civic-location elin } identifier id network-policy profile [profile-num] power-over-ethernet } }</pre>	
	<pre>no lldp tlv-enable { basic-tlv { all port-description system-capability system-description system-name } dot1-tlv { all port-vlan-id protocol-vlan-id vlan-name } dot3-tlv { all link-aggregation mac-physic max-frame-size power } med-tlv { all capability inventory location { civic-location elin } identifier id network-policy profile [profile-num] power-over-ethernet } }</pre>	

Parameter	Parameter	Description
Description	basic-tlv	Basic management TLV
	port-description	Port Description TLV
	system-capability	System Capabilities TLV
	system-description	System Description TLV
	system-name	System Name TLV
	dot1-tlv	802.1 organizationally specific TLV
	port-vlan-id	Port VLAN ID TLV
	protocol-vlan-id	Port And Protocol VLAN ID TLV
	vlan-id	VLAN ID
	vlan-name	VLAN Name TLV
	vlan-id	VLAN ID corresponding to the specified VLAN name
	dot3-tlv	802.3 organizationally specific TLV
	link-aggregation	Link Aggregation TLV
	mac-physic	MAC/PHY Configuration/Status TLV
	max-frame-size	Maximum Frame Size TLV
	power	Power Via MDI TLV
	med-tlv	LLDP MED TLV
	capability	LLDP-MED Capabilities TLV
	inventory	Inventory management TLVs, including hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.
	location	Location Identification TLV
	civic-location	Common address information about the network device in location identification TLVs.
	elin	Encapsulated emergency number
	id	Policy ID
	network-policy	Network Policy TLV
	profile-num	ID of network policy
	power-over-ethernet	Extended Power-via-MDI TLV
Defaults	By default, all TLVs other than Location Identification TLV can be advertised on the interface for products other than S12000. For the S12000 product series, only basic TLVs and IEEE 802.1 TLVs are advertised. To advertise IEEE 802.3 TLVs and LLDP-MED TLVs, run the lldp tlv-enable command.	
Command Mode	Interface configuration mode	
Usage Guide	During configuration of basic management TLVs, IEEE 802.1 TLVs, and IEEE 802.3 TLVs, if the all parameter is specified, all optional TLVs of the types are advertised. During configuration of LLDP-MED TLVs, if the all parameter is specified, all LLDP-MED TLVs except Location Identification TLVs are advertised. When configuring LLDP-MED Capability TLVs, configure LLDP-MED MAC/PHY TLVs first. When canceling	

	LLDP-MED MAC/PHY TLVs, cancel LLDP-MED Capability TLVs first. When configuring LLDP-MED TLVs, configure LLDP-MED Capability TLVs first so that LLDP-MED TLVs of other types can be configured. To cancel LLDP-MED TLVs, cancel LLDP-MED TLVs of other types first so that LLDP-MED Capability TLVs can be canceled.					
Configuration Examples	The following example configures all IEEE 802.1 TLVs to be advertised. <pre>FS# configure terminal FS(config)#interface gigabitethernet 0/1 FS(config-if-GigabitEthernet 0/1)#lldp tlv-enable dot1-tlv all</pre> The following example applies LLDP network policy 1 on the 0/1 interface. <pre>FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv network-policy profile 1</pre> The following example applies the LLDP Civic Address (ID: 1) configuration on the 0/1 interface. <pre>FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if-GigabitEthernet 0/1)#lldp tlv-enable med-tlv location civic-location identifier 1</pre> The following example applies the emergency number (ID: 1) on the 0/1 interface. <pre>FS#config FS(config)#interface gigabitethernet 0/1 FS(config-if-GigabitEthernet 0/1)#lldp location elin identifier 1</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show lldp tlv-config interface</td><td>Displays the attributes of advertisable TLVs</td></tr></table>	Command	Description	show lldp tlv-config interface	Displays the attributes of advertisable TLVs	
Command	Description					
show lldp tlv-config interface	Displays the attributes of advertisable TLVs					
Platform Description	N/A					

9.22 show lldp local-information

	Use this command to display the LLDP information of local device. The information will be encapsulated in the TLVs and sent to the neighbor device.	
	show lldp local-information [global interface <i>interface-name</i>]	
Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
Defaults	N/A	
Command	Privileged EXEC mode	

Mode	
Usage Guide	global parameter: display the global LLDP information to be sent. Interface parameter: displays the LLDP information to be sent out the interface specified. No parameter: display all LLDP information, including global and interface-based LLDP information.
Configuration Examples	The following example displays the device information to be sent to neighbor device. <pre> FS# show lldp local-information Global LLDP local-information: Chassis ID type : MAC address Chassis id : 00d0.f822.33aa System name : System name System description : System description System capabilities supported : Repeater, Bridge, Router System capabilities enabled : Repeater, Bridge, Router LLDP-MED capabilities : LLDP-MED Capabilities, Network Policy, Location Identification, Extended Power via MDI-PD, Inventory Device class : Network Connectivity HardwareRev : 1.0 FirmwareRev : SoftwareRev : FSOS 10.4(3) Release(94786) SerialNum : 1234942570001 Manufacturer name : Manufacturer name Asset tracking identifier : ----- Lldp local-information of port [GigabitEthernet 0/1] ----- Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : Management address subtype : 802 mac address Management address : 00d0.f822.33aa Interface numbering subtype : Interface number : 0 Object identifier : 802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 </pre>

PPVID Supported : YES
 PPVID Enabled : NO
 VLAN name of VLAN 1 : VLAN0001
 Protocol Identity :

802.3 organizationally information

Auto-negotiation supported : YES
 Auto-negotiation enabled : YES
 PMD auto-negotiation advertised : 100BASE-TX full duplex mode, 100BASE-TX half duplex mode
 Operational MAU type :
 PoE support : NO
 Link aggregation supported : YES
 Link aggregation enabled : NO
 Aggregation port ID : 0
 Maximum frame Size : 1500

LLDP-MED organizationally information

Power-via-MDI device type : PD
 Power-via-MDI power source : Local
 Power-via-MDI power priority :
 Power-via-MDI power value :
 Model name : Model name

show lldp local-information command output description:

Field	Description
Chassis ID type	Chassis ID type for identifying the Chassis ID field
Chassis ID	Used to identify the device, and is generally represented with MAC address
System name	Name of the sending device
System description	Description of the sending device, including hardware/software version, operating system and etc.
System capabilities supported	Capabilities supported by the system
System capabilities enabled	Capabilities currently enabled by the system
LLDP-MED capabilities	LLDP-MED capabilities supported by the system
Device class	MED device class, which is divided into 2 categories: network connectivity device and terminal device. Network connectivity device Class I: normal terminal device Class II: media terminal device; besides Class I capabilities, it also supports media streams. Class III: communication terminal device; it supports all the capabilities of Class I and Class II and IP communication.

	HardwareRev	Hardware version
	FirmwareRev	Firmware version
	SoftwareRev	Software version
	SerialNum	Serial number
	Manufacturer name	Device manufacturer
	Asset tracking identifier	Asset tracking ID
	Port ID type	Port ID type
	Port ID	Port ID
	Port description	Port description
	Management address subtype	Management address type
	Management address	Management address
	Interface numbering subtype	Type of the interface identified by the management address
	Interface number	ID of the interface identified by the management address
	Object identifier	ID of the object identified by the management address
	Port VLAN ID	Port VLAN ID
	Port and protocol VLAN ID	Port and Protocol VLAN ID
	PPVID Supported	Indicates whether port and protocol VLAN is supported
	PPVID Enabled	Indicates whether port and protocol VLAN is enabled
	VLAN name of VLAN 1	Name of VLAN 1
	Protocol Identity	Protocol identifier
	Auto-negotiation supported	Indicates whether auto-negotiation is supported
	Auto-negotiation enabled	Indicates whether auto-negotiation is enabled
	PMD auto-negotiation advertised	Auto-negotiation advertising capability of the port
	Operational MAU type	Speed and duplex state of the port
	PoE support	Indicates whether POE is supported
	Link aggregation supported	Indicates whether link aggregation is supported
	Link aggregation enabled	Indicates whether link aggregation is enabled
	Aggregation port ID	ID of the link aggregation port
	Maximum frame Size	Maximum frame size supported by the port
	Power-via-MDI device type	Device type, including: PSE (power sourcing equipment) PD (powered device)
	Power-via-MDI power source	Power source type
	Power-via-MDI power priority	Power supply priority
	Power-via-MDI power value	Available power on port
	Model name	Name of model
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.23 show lldp location

	Use this command to display the common LLDP address or emergency number of the local device.	
	show lldp location { civic-location elin-location } { identifier <i>id</i> interface <i>interface-name</i> static }	
Parameter	Parameter	Description
Description	civic-location	Encapsulates a common address of a network device.
	elin-location	Encapsulates an emergency number.
	identifier	Displays one address or emergency number configured.
	id	Policy ID of configured information
	interface	Displays the address or emergency number on an interface.
	interface-name	Interface name
	static	Displays all addresses or emergency numbers configured.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If the policy ID is specified, the specified address or emergency number is displayed. If the interface name is specified, the address or emergency number configured on the interface is displayed. If no parameter is specified, all addresses or emergency numbers are displayed.	
Configuration Examples	The following example displays all addresses. <pre> FS# show lldp location civic-location static LLDP Civic location information ----- Identifier : testt County : china City Division : 22 Leading street direction : 44 Street number : 68 Landmark : 233 Name : liuy Building : 19bui Floor : 1 Room : 33 City : fuzhou Country : 86 Additional location : aaa Ports : Gi0/1 ----- Identifier : tee </pre>	

	----- The following example displays all emergency numbers. FS# show lldp location elin-location static Elin location information ----- Identifier : t Elin : iiii iiiii Ports : Gi1/0/3 -----	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.24 show lldp neighbors

	Use this command to display the LLDP information about a neighboring device.	
	show lldp neighbors [interface <i>interface-name</i>] [detail]	
Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
	detail	All information about a neighboring device
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If the detail parameter is not specified, the brief information about a neighboring device is displayed. If the detail parameter is specified, the detailed information about a neighboring device is displayed. If the interface parameter is specified, the neighboring device information received on the specified interface is displayed.	
Configuration Examples	The following example displays the neighboring device information received on all ports. FS# show lldp neighbors detail Lldp neighbor-information of port [GigabitEthernet 0/1] Neighbor index : 1 Device type : LLDP Device Update time : 1 hour 53minutes 30seconds	

```

Aging time           : 5seconds

Chassis ID type      : MAC address
Chassis id           : 00d0.f822.33cd
System name          : System name
System description    : System description
System capabilities supported : Repeater, Bridge, Router
System capabilities enabled : Repeater, Bridge, Router

Management address subtype : 802 mac address
Management address      : 00d0.f822.33cd
Interface numbering subtype :
Interface number         : 0
Object identifier        :

LLDP-MED capabilities    :
Device class             :
HardwareRev              :
FirmwareRev              :
SoftwareRev              :
SerialNum                :
Manufacturer name        :
Asset tracking identifier :

Port ID type            : Interface name
Port id                 : GigabitEthernet 0/1
Port description         :

802.1 organizationally information
Port VLAN ID            : 1
Port and protocol VLAN ID (PPVID) : 1
PPVID Supported          : YES
PPVID Enabled            : NO
VLAN name of VLAN 1     : VLAN0001
Protocol Identity        :

802.3 organizationally information
Auto-negotiation supported : YES
Auto-negotiation enabled  : YES
PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX
half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
Operational MAU type     : speed(1000)/duplex(Full)
PoE support               : NO
Link aggregation supported : YES

```

Link aggregation enabled : NO
 Aggregation port ID : 0
 Maximum frame Size : 1500
 LLDP-MED organizationally information
 Power-via-MDI device type :
 Power-via-MDI power source :
 Power-via-MDI power priority :
 Power-via-MDI power value :

Description of fields:

Field	Description
Neighbor index	Neighbor index
Device type	Type of neighboring device
Update time	Latest update time of neighbor information
Aging time	Aging time of a neighbor, namely the time after which a neighbor is aged and deleted
Chassis ID type	Chassis ID type
Chassis ID	Used to identify a device. Usually, a MAC address is used.
System name	Device name
System description	Device description, including hardware/software version and operating system
System capabilities supported	Functions supported by the system
System capabilities enabled	Functions enabled by the system
Management address subtype	Type of management address
Management address	Management address
Interface numbering subtype	Interface type of management address
Interface number	Interface ID of management address
Object identifier	Object ID of management address
Device class	MED device type: network connectivity device and terminal device Network connectivity device: Class I: general terminal device Class II: media terminal device, including capabilities of Class I and supporting media stream Class III: communication terminal device, including capabilities of Class I and Class II and supporting IP communication
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Manufacturer name
Asset tracking identifier	Asset ID
Port ID type	Port ID type
Port ID	Port ID

	Port description	Port description
	Port VLAN ID	VLAN ID of a port
	Port and protocol VLAN ID	Port and protocol VLAN ID
	PPVID Supported	Whether port and protocol VLAN is supported
	PPVID Enabled	Whether port and protocol VLAN is enabled
	VLAN name of VLAN 1	VLAN 1 name
	Protocol Identity	Protocol ID
	Auto-negotiation supported	Whether auto-negotiation is supported
	Auto-negotiation enabled	Whether auto-negotiation is enabled
	PMD auto-negotiation advertised	Port auto-negotiation advertisement capability
	Operational MAU type	Rate and duplex status of port auto-negotiation
	PoE support	Whether POE is supported
	Link aggregation supported	Whether link aggregation is supported
	Link aggregation enabled	Whether link aggregation is enabled
	Aggregation port ID	ID of link aggregation port
	Maximum frame Size	Maximum frame length supported by a port
	Power-via-MDI device type	Device type, including: PSE PD
	Power-via-MDI power source	Power type
	Power-via-MDI power priority	Power supply priority
	Power-via-MDI power value	Power value of a port where power is supplied
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.25 show lldp network-policy profile

	Use this command to display the information about an LLDP network policy.	
	show lldp network-policy { profile [<i>profile-num</i>] interface <i>interface-name</i> }	
Parameter Description	Parameter	Description
	<i>profile-num</i>	ID of a network policy, in the range from 1 to 1024.
	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	If <i>profile-num</i> is specified, the information about the specified network policy is displayed. If no parameter is specified, the information about all network policies is displayed.	
Configuration Examples	The following example displays the information about a network policy. FS# show lldp network-policy profile network-policy information: ----- Network Policy Profile 1 voice vlan 2 cos 4 dscp 6 voice-signaling vlan 2000 cos 4 dscp 6	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.26 show lldp statistics

	The following example displays LLDP statistics.	
	show lldp statistics [global interface <i>interface-name</i>]	
Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	global parameter: display the global LLDP statistics. Interface parameter: display the LLDP statistics of the specified interface.	
Configuration Examples	The following example displays all LLDP statistics. FS# show lldp statistics lldp statistics global Information: Neighbor information last changed time : 1hour 52minute 22second The number of neighbor information inserted : 2 The number of neighbor information deleted : 0 The number of neighbor information dropped : 0 The number of neighbor information age out : 1	

```
-----
Lldp statistics information of port [GigabitEthernet 0/1]
-----
```

```
The number of lldp frames transmitted   : 26
The number of frames discarded          : 0
The number of error frames              : 0
The number of lldp frames received      : 12
The number of TLVs discarded            : 0
The number of TLVs unrecognized         : 0
The number of neighbor information aged out : 0
```

show lldp statistics command output description:

Field	Description
Neighbor information last change time	Time the neighbor information is latest updated
The number of neighbor information inserted	Number of times of adding neighbor information
The number of neighbor information deleted	Number of times of removing neighbor information
The number of neighbor information dropped	Number of times of dropping neighbor information
The number of neighbor information aged out	Number of the neighbor information entries that have aged out
The number of lldp frames transmitted	Total number of the LLDPDUs transmitted
The number of frames discarded	Total number of the LLDPDUs discarded
The number of error frames	Total number of the LLDP error frames received
The number of lldp frames received	Total number of the LLDPDUs received
The number of TLVs discarded	Total number of the LLDP TLVs dropped
The number of TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized
The number of neighbor information aged out	Number of the neighbor information entries that have aged out

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.27 show lldp status

	Use this command to display LLDP status information.									
	show lldp status [interface <i>interface-name</i>]									
Parameter	Parameter	Description								
Description	<i>interface-name</i>	Interface name								
Defaults	N/A									
Command Mode	Privileged EXEC mode									
Usage Guide	interface parameter: display the LLDP status information of the specified interface.									
Configuration Examples	The following example displays LLDP status information of all ports. <pre>FS# show lldp status Global status of LLDP : Enable Neighbor information last changed time : 1hour 52minute 22second Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 3 ----- Port [GigabitEthernet 0/1] ----- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 1 Number of MED neighbors : 0</pre> show lldp status command output description: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Global status of LLDP</td><td>Whether LLDP is globally enabled</td></tr><tr><td>Neighbor information last changed time</td><td>Time the neighbor information is latest updated</td></tr><tr><td>Transmit interval</td><td>LLDPDU transmit interval</td></tr></table>		Field	Description	Global status of LLDP	Whether LLDP is globally enabled	Neighbor information last changed time	Time the neighbor information is latest updated	Transmit interval	LLDPDU transmit interval
Field	Description									
Global status of LLDP	Whether LLDP is globally enabled									
Neighbor information last changed time	Time the neighbor information is latest updated									
Transmit interval	LLDPDU transmit interval									

	Hold multiplier Reinit delay Transmit delay Notification interval Fast start counts Port status of LLDP Port state Port encapsulation Operational mode Notification enable Error detect enable Number of neighbors Number of MED neighbors	TTL multiplier Port re-initialization delay LLDPDU transmit delay Interval for sending LLDP Traps The number of fast sent LLDPDUs Whether LLDP is enabled on the port Link status of port: UP or DOWN LLDPDU encapsulation format Operating mode of LLDP Whether LLDP Trap is enabled on the port Whether error detection is enabled on the port Number of neighbors Number of MED neighbors
Related Commands	Command N/A	Description N/A
Platform Description	N/A	

9.28 show lldp tlv-config

	Use this command to display the advertisable TLV configuration of a port.	
	show lldp tlv-config [interface <i>interface-name</i>]	
Parameter Description	Parameter <i>interface-name</i>	Description Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Interface parameter: display the LLDP TLV configuration of the specified interface.	
Configuration Examples	The following example displays TLV information of port 1. <pre> FS# show lldp tlv-config interface GigabitEthernet 0/1 LLDP tlv-config of port [GigabitEthernet 0/1] ----- NAME STATUS DEFAULT ----- Basic optional TLV: Port Description TLV YES YES </pre>	

	System Name TLV YES YES System Description TLV YES YES System Capabilities TLV YES YES Management Address TLV YES YES IEEE 802.1 extend TLV: Port VLAN ID TLV YES YES Port And Protocol VLAN ID TLV YES YES VLAN Name TLV YES YES IEEE 802.3 extend TLV: MAC-Physic TLV YES YES Power via MDI TLV YES YES Link Aggregation TLV YES YES Maximum Frame Size TLV YES YES LLDP-MED extend TLV: Capabilities TLV YES YES Network Policy TLV YES YES Location Identification TLV NO NO Extended Power via MDI TLV YES YES Inventory TLV YES YES	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.29 { voice | voice-signaling } vlan

	Use this command to configure the LLDP network policy. Use the no form of this command to delete the policy.	
	{ voice voice-signaling } vlan { { <i>vlan-id</i> [cos <i>cvalue</i> dscp <i>dvalue</i>] } { dot1p [cos <i>cvalue</i> dscp <i>dvalue</i>] } none untagged }	
	no { voice voice-signaling } vlan	
Parameter Description	Parameter	Description
	voice	Voice application
	voice-signaling	Voice-signaling application
	vlan-id	(Optional) VLAN ID of voice flow. The value ranges from 1 to 4094.
	cos	(Optional) Class of service
	cvalue	(Optional) CoS of the configured voice flow. The value ranges from 0 to 7, and the default value is 5 .
	dscp	(Optional) Differentiated services code point

	dvalue	(Optional) DSCP value of the configured voice flow. The value ranges from 0 to 63. The default value is 46.
	dot1p	(Optional) 802.1p priority tagging. The tag frame includes user_priority and vlan id is 0.
	none	(Optional) The network policy is not advertised. VoIP determines the network policy based on its configuration.
	untagged	(Optional) The untag frame is sent in the voice vlan in VoIP. In this case, the value of vlan id and cos are ignored.
Defaults	N/A	
Command Mode	LLDP network policy configuration mode	
Usage Guide	In the LLDP network policy configuration mode, configure the LLDP network policy.	
Configuration Examples	The following example configures the LLDP network policy (profile-num is 1). FS#config FS(config)#lldp network-policy profile 1 FS(config-lldp-network-policy)# voice vlan untagged FS(config-lldp-network-policy)# voice-signaling vlan 3 cos 4 FS(config-lldp-network-policy)# voice-signaling vlan 3 dscp 6	
Related Commands	Command	Description
	show lldp network-policy profile [<i>profile-num</i>]	Displays the LLDP network policy.
Platform Description	N/A	

10 QinQ Commands

10.1 dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value

	Use this command to map the priority from the outer tag to the inner tag for the packets on the interface. Use the no form of this command to restore the default setting.	
	dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value	
	no dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value	
	default dot1q-tunnel cos inner-cos-value remark-cos outer-cos-value	
Parameter	Parameter	Description
Description	<i>inner-cos-value</i>	Indicates the CoS value of the inner tag.
	<i>outer-cos-value</i>	Indicates the CoS value of the outer tag.
	no	Cancels the priority mapping of the packets on the interface.
Defaults	The policy list is null by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If the QoS policy based on the COS value is set for the service provider's network to which a user network connects, the COS value of the outer tag can be set to different values based on the data packet importance. In this case, important services can be preferentially processed and transmitted.	
Configuration Examples	The following example configures the priority mapping from the outer tag to the inner tag. <pre> FS# configure FS(config)# interface gigabitEthernet 0/2 FS(config-if)# dot1q-tunnel cos 3 remark-cos 5 FS(config-if)# end </pre>	
Related Commands	Command	Description
	show interface intf-name remark	N/A
Platform Description	N/A	

10.2 frame-tag tpid

	Use this command to set the packet TPID compatible with the manufacturer TPID. Use the no or default form of this command to restore the default setting.
	frame-tag tpid tpid
	no frame-tag tpid
	default frame-tag tpid

Parameter Description	Parameter	Description
	tpid	Packet TPID.
Defaults	The default is 0x8100.	
Command Mode	Interface configuration mode.	
Usage Guide	If the TPID value of the connected third-party device is not 0x8100 (default value) defined in IEEE802.1Q, the TPID value on the egress used to connect to the third-party device is the TPID value of the third-party device.	
Configuration Examples	The following example sets the packet TPID compatible with the manufacturer TPID. <pre> FS(config)# interface g0/3 FS(config-if)# frame-tag tpid 0x9100 FS(config-if)# end FS# show frame-tag tpid Port tpid ----- Gi0/3 0x9100 </pre>	
Related Commands	Command	Description
	show frame-tag tpid	N/A
Platform Description	N/A	

10.3 inner-priority-trust enable

	Use this command to copy the priority of the inner tag to the outer tag of the packets on the interface. Use the no or default form of this command to restore the default setting.	
	inner-priority-trust enable	
	no inner-priority-trust enable	
	default inner-priority-trust enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	

Usage Guide	If the QoS policy is configured based on the COS value of the user's VLAN tag for the service provider's network to which a user network connects, the user's VLAN tag priority can be copied to the outer VLAN tag, so that the user's packets are encapsulated with the outer VLAN tag and have the same priority as the user's VLAN tag. In this case, the user's packets can be preferentially processed and transmitted on the service provider's network.	
Configuration Examples	The following example copies the priority of the inner tag to the outer tag of the packets on the interface. <pre>FS#configure terminal FS(config)# interface gigabitEthernet 0/2 FS(config-if)# inner-priority-trust enable FS(config-if)#end</pre>	
Related Commands	Command	Description
	show inner-priority-trust	N/A
Platform Description	N/A	

10.4 l2protocol-tunnel

	Use this command to set the dot1q-tunnel port to receive L2 protocol message. Use the no or default form of this command to disable this function.	
	l2protocol-tunnel { stp gvrp }	
	no l2protocol-tunnel { stp gvrp }	
	default l2protocol-tunnel { stp gvrp }	
Parameter Description	Parameter	Description
	stp	Receives stp message.
	gvrp	Receives gvrp message.
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	If the STP and GVRP packets need to be transparently transmitted, this function must be enabled in global configuration mode.	
Configuration Examples	The following example enables the function of receiving L2 protocol gvrp and stp. <pre>FS#configure FS(config)# l2protocol-tunnel stp FS(config)# l2protocol-tunnel gvrp FS(config)#end</pre>	

Related Commands	Command	Description
	show l2protocol-tunnel { gvrp stp }	N/A
Platform Description	N/A	

10.5 l2protocol-tunnel enable

	Use this command to enable transparent transmission of L2 protocol message. Use the no or default form of this command to restore the default setting.	
	l2protocol-tunnel { stp gvrp } enable	
	no l2protocol-tunnel { stp gvrp } enable	
Parameter Description	Parameter	Description
	stp	Transparently transmits stp message.
	gvrp	Transparently transmits gvrp message.
Defaults	It is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If this function is enabled in global and interface configuration modes, STP packets can be transparently transmitted after the bridge-frame forwarding protocol bpdu command is enabled in global configuration mode.	
Configuration Examples	Here is an example of enabling transparent transmission of L2 protocol message : <pre> FS#configure FS(config)# interface fa 0/1 FS(config-if)# l2protocol-tunnel gvrp enable FS(config-if)#end </pre>	
Related Commands	Command	Description
	show l2protocol-tunnel { gvrp stp }	N/A
Platform Description	N/A	

10.6 l2protocol-tunnel tunnel-dmac

	Use this command to set the MAC address for the transparent transmission of the corresponding protocol messages. Use the no or default form of this command to restore the default setting.

	l2protocol-tunnel { stp gvrp } tunnel-dmac mac-address	
	no l2protocol-tunnel { stp gvrp } tunnel-dmac mac-address	
	default l2protocol-tunnel { stp gvrp } tunnel-dmac mac-address	
Parameter Description	Parameter	Description
	stp	Sets the STP transparent transmission address.
	gvrp	Sets the GVRP transparent transmission address.
Defaults	The first three bytes of the address are 01d0f8 and the last three bytes are 000005 for stp and 000006 for gvrp by default.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the MAC address for the L2-protocol transparent transmission function: <pre>FS# configure terminal FS(config-if)# l2protocol-tunnel gvrp tunnel-dmac 011AA9 000005 FS(config-if)#end</pre>	
Related Commands	Command	Description
	show l2protocol-tunnel { gvrp stp }	N/A
Platform Description	N/A	

10.7 show dot1q-tunnel

	Use this command to display whether dot1q-tunnel of interface is enabled or not.	
	show dot1q-tunnel [interfaces intf-id]	
Parameter Description	Parameter	Description
	intf-id	The specified interface.
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	

Configuration Examples	The following example displays whether dot1q-tunnel of interface is enabled or not.	
	<pre> FS# show dot1q-tunnel Ports Dot1q-tunnel ----- Gi0/1 Enable </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description		

10.8 show frame-tag tpid

	Use this command to display the configuration of interface tpid.	
	show frame-tag tpid [interfaces <i>intf-id</i>]	
Parameter Description	Parameter	Description
	<i>intf-id</i>	Specifies the interface.
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration of interface tpid.	
	<pre> FS# show frame-tag tpid Ports tpid ----- Gi0/1 0x9100 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.9 show inner-priority-trust

	Use this command to display whether the priority copy function is enabled.	
	show inner-priority-trust	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	
Configuration Examples	The following example displays whether the priority copy function is enabled. <pre>FS# show inner-priority-trust Port inner-priority-trust ---- - Gi0/1 enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description		

10.10 show interfaces dot1q-tunnel

	Use this command to display the VLAN configuration on the dot1q-tunnel port.	
	show interfaces [<i>intf-id</i>] dot1q-tunnel	
Parameter Description	Parameter	Description
	intf-id	Specifies the interface.
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	

Configuration	The following example displays the VLAN configuration on the dot1q-tunnel port.	
Examples	<pre>FS# show interfaces dot1q-tunnel Interface: Gi0/3 Native vlan: 10 Allowed vlan list: 4-6, 10, 30-60 Tagged vlan list: 4, 6, 30-60</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.11 show interfaces remark

	Use this command to display the priority mapping configuration.											
	show interfaces [<i>intf-id</i>] remark											
Parameter Description	Parameter	Description										
	<i>intf-id</i>	specifies an interface										
Defaults	N/A											
Command Mode	Any mode											
Usage Guide	N/A											
Configuration Examples	The following example displays the priority mapping configuration. FS# show interfaces remark <table><tr><th>Ports</th><th>Type</th><th>From value</th><th>To value</th></tr><tr><td>Gi0/1</td><td>Cos-To-Cos</td><td>3</td><td>5</td></tr></table>				Ports	Type	From value	To value	Gi0/1	Cos-To-Cos	3	5
Ports	Type	From value	To value									
Gi0/1	Cos-To-Cos	3	5									
Related Commands	Command		Description									
	N/A		N/A									
Platform Description	N/A											

10.12 show l2protocol-tunnel

	Use this command to display transparent transmission configuration of L2 protocol.	
	show l2protocol-tunnel { gvrp stp }	
Parameter Description	Parameter	Description
	gvrp	Displays configuration of transparently transmitting gvrp protocol.
	stp	Displays configuration of transparently transmitting stp protocol.
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	
Configuration Examples	The following example displays transparent transmission configuration of L2 protocol. <pre>FS# show l2protocol-tunnel stp L2protocol-tunnel: Stp Enable FS# show l2protocol-tunnel gvrp L2protocol-tunnel: gvrp Disable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.13 show registration-table

	Use this command to display vid add policy list of protocol-based dot1q-tunnel port.	
	show registration-table [interfaces intf-id]	
Parameter Description	Parameter	Description
	intf-id	Specifies the interface.
Defaults	N/A	
Command Mode	Any mode	

Usage Guide	N/A	
Configuration Examples	The following example displays vid add policy list of protocol-based dot1q-tunnel port. <pre> FS# show registration-table Ports Type Outer-VID Inner-VID-list ----- Gi0/7 Add-outer 5 7-10,15,20-30 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.14 show traffic-redirect

	Use this command to display flow-based vid change or add policy list.	
	show traffic-redirect [interfaces <i>intf-id</i>]	
Parameter Description	Parameter	Description
	intf-id	Specifies the interface.
Defaults	N/A	
Command Mode	Any mode	
Usage Guide	N/A	
Configuration Examples	The following example displays flow-based vid change or add policy list. <pre> FS# show traffic-redirect Ports Type VID Match-filter ----- Gi0/3 Mod-outer 23 11 Gi0/3 Mod-outer 3 4 Gi0/3 Mod-outer 6 5 Gi0/3 Mod-inner 8 inner-to-8 Gi0/6 Mod-inner 9 100 Gi0/7 Nested-vid 13 nest-13 </pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.15 show translation-table

	Use this command to display vid modify policy list of prorocol-based access, trunk, hybrid port.				
	show translation-table [interfaces <i>intf-id</i>]				
Parameter Description	Parameter		Description		
	intf-id		Specifies the interface.		
Defaults	N/A				
Command Mode	Any mode				
Usage Guide	N/A				
Configuration Examples	The following example displays vid modify policy list of prorocol-based access, trunk, hybrid port.				
	FS# show translation-table				
	Ports	Type	Relay-VID	Old-local	Local\inner-VID-list

	Gi0/7	Inner-CVID 8		N/A	10-20
	Gi0/7	Local-SVID 1001		N/A	30-60
	Gi0/7	In+Out	8	20	50
Related Commands	Command			Description	
	N/A			N/A	
Platform Description	N/A				

10.16 switchport dot1q-tunnel allowed vlan

	Use this command to configure the allowed VLAN of dot1q-tunnel. Use the no or default form of this command to restore the default setting.
	switchport dot1q-tunnel allowed vlan { [add] tagged <i>vlist</i> [add] untagged <i>vlist</i> remove <i>vlist</i> }
	no switchport dot1q-tunnel allowed vlan

	default switchport dot1q-tunnel allowed vlan	
Parameter Description	Parameter	Description
	add	Add allowed VLAN.
	tagged	Tag-carried.
	untagged	Not tag-carried.
	<i>v_list</i>	vlan id list.
	no	Remove the settings.
Defaults	The default is untagged 1 .	
Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies vlan 3-6 of dot1q-tunnel port as allowed VLAN and outputting the frame with tag. <pre>FS(config)#interface gigabitEthernet 0/1 FS(config-if)#switchport dot1q-tunnel allowed vlan tagged 3-6 FS(config)#end</pre>	
Related Commands	Command	Description
	show interface dot1q-tunnel	N/A
Platform Description	N/A	

10.17 switchport dot1q-tunnel native vlan

	Use this command to configure the default vlan id of dot1q-tunnel. Use the no or default form of this command to restore the default setting.	
	switchport dot1q-tunnel native vlan <i>vid</i>	
	no switchport dot1q-tunnel native vlan default switchport dot1q-tunnel native vlan	
Parameter Description	Parameter	Description
	<i>vid</i>	Configures default vlan id.
Defaults	The default is VLAN 1.	

Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies default VLAN of dot1q-tunnel port as 8. FS(config)#interface gigabitEthernet 0/1 FS(config-if)#switchport dot1q-tunnel native vlan 8 FS(config)#end	
Related Commands	Command	Description
	show interface dot1q-tunnel	N/A
Platform Description	N/A	

10.18 switchport mode dot1q-tunnel

	Use this command to configure the interface as the dot1q-tunnel interface. Use the no or default form of this command to restore the default setting.	
	switchport mode dot1q-tunnel	
	no switchport mode default switchport mode	
Parameter Description	Parameter	Description
	-	-
Defaults	The interface is not a tunnel port by default.	
Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the interface as the dot1q-tunnel interface. FS(config)# interface gigabitEthernet 0/1 FS(config-if)# switchport mode dot1q-tunnel FS(config)# end	
Related Commands	Command	Description
	show vlan	N/A
Platform Description	N/A	

11 ERPS Commands

11.1 associate sub-ring

	Use this command to associate the ethernet ring with its sub-rings.	
	associate sub-ring raps-vlan <i>vlan-list</i>	
	no associate sub-ring raps-vlan <i>vlan-list</i>	
Parameter Description	Parameter	Description
	<i>vlan-list</i>	Sub-rings' R-APS VLAN.
Defaults	By default, Ethernet ring is not associated with its sub-rings.	
Command Mode	ERPS configuration mode.	
Usage Guide	1. You need to configure this command on all nodes of the Ethernet ring, so as to transmit its sub-ring's ERPS protocol packets in the Ethernet ring. 2. Configuring the association is mainly to make the sub-ring's protocol packets transmit in the Ethernet ring. Users can also adopt the configuration command provided by the VLAN module to configure elaborately the VLAN and the relation between ports and VLAN, so as to transmit the sub-ring's protocol packets in other Ethernet rings and not leak the packets to the user network.	
Configuration Examples	The following example associates the Ethernet sub-ring with other Ethernet rings: <pre>#Enter the privileged EXEC mode FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Configure the link mode of the Ethernet ring port and the default VLAN. FS(config)# interface fastEthernet 0/1 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# interface fastEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# exit # Enter the erps configuration mode. FS(config)# erps raps-vlan 4093 #Add the ports that participate in the ERPS protocol computing to the Ethernet ring. FS(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2 # Configure the Ethernet subring</pre>	

	<pre> FS(config)# erps raps-vlan 100 FS(config)# interface fastEthernet 0/3 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# erps raps-vlan 100 FS(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel FS(config-if)# exit # Associate the subring with other Ethernet rings. FS(config)# erps raps-vlan 4093 FS(config-erps4093)# associate sub-ring raps-vlan 100 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.2 erps enable

	Use this command to enable/disable the ERPS function in the global configuration mode.	
	erps enable	
	no erps enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Disabled	
Command Mode	Global configuration mode.	
Usage Guide	The ERPS protocol of the specified ring will begin running truly only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled.	
Configuration Examples	The following example enables the ERPS protocol globally: <pre> # Enter the privileged EXEC mode FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Enable the ERPS function globally. </pre>	

	<pre>FS(config)# erps enable</pre> <pre># Enter the ERPS configuration mode</pre> <pre>FS(config)# erps raps-vlan 4093</pre> <pre># Enable the ERPS function for the specified ring.</pre> <pre>FS(config-erps4093)# state enable</pre>	
Related Commands	Command	Description
	state enable	After entering the ERPS configuration mode of the specified ring, configure this command to enable the ERPS protocol of this specified ring.
Platform Description	N/A	

11.3 erps monitor link-state by oam

	Use this command to configure the method of monitoring the ERPS link state.	
	erps monitor link-state by oam vlan <i>vlan-id</i>	
	no erps monitor link-state by oam	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, it adopts the directly monitoring the link physical state (up or down) rather than the oam method.	
Command Mode	Global configuration mode.	
Usage Guide	For the link state monitoring, use the method of directly monitoring the link physical state (up or down), also monitor the logic state (unidirectional fault, bidirectional fault or normal) of the link by the OAM. By default, the former is adopted. If the OAM method is used, the inefficient link state monitoring may cause the convergence time longer when the topology changes.	
Configuration Examples	The following example configures the method of monitoring the link state. <pre># Enter the privileged EXEC mode.</pre> <pre>FS# configure terminal</pre> Enter configuration commands, one per line. End with CNTL/Z. <pre># Configure the method of monitoring the link state.</pre> <pre>FS(config)# erps monitor link-state by oam vlan 100</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.4 erps raps-vlan

	Use this command to configure the R-APS VLAN of Ethernet ring.	
	erps raps-vlan <i>vlan-id</i>	
	no erps raps-vlan <i>vlan-id</i>	
Parameter Description	Parameter	Description
	vlan-id	R-APS VLAN ID
Defaults	No R-APS VLAN is configured.	
Command Mode	Global configuration mode.	
Usage Guide	The R-APS VLAN must be the VLAN that is not used on the device. Cannot set the VLAN1 to the R-APS VLAN. The same Ethernet ring of different devices needs the same R-APS VLAN. If you want to transparently transmit the ERPS protocol packets on a device without the ERPS function configured, make sure that only the two ports connected to the Ethernet ring on this device allow the R-APSA VLAN packets corresponding to this ERPS ring passing through. Otherwise, the other VLAN packets may enter the R-APS VLAN through the transparent transmission, causing the shock to the ERPS ring.	
Configuration Examples	<pre># Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. #Configure the R-APS VLAN globally. FS(config)# erps raps-vlan 4093</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.5 protected-instance

	Use this command to configure the VLAN protected by the Ethernet ring to implement the load balance function.	
	protected-instance <i>instance-id-list</i>	
	no protected-instance	
Parameter Description	Parameter	Description
	instance-id-list	Instance protected by this Ethernet ring. (The VLANs corresponding to these instances are the VLANs protected by the Ethernet ring.)
Defaults	By default, all VLANs are protected.	
Command Mode	EPRS configuration mode.	
Usage Guide	The protected VLAN consists of the R-APS VLAN of this Ethernet ring and the data VLAN protected by this Ethernet ring.	
Configuration Examples	Suppose that the ERP1 and ERP2 are configured on the switch to implement the load balance. The R-APS VLAN of the ERPS1 is 100, the protected data VLAN is in the range of 1 to 99 and 101-2000, the R-APS VLAN of the ERPS2 is 4093, and the protected data VLAN is in the range of 2001 to 4092 and 4094. Configuration for the load balance is shown as below: <pre># Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Configure the VLAN configured by the ERP1. FS(config)# spanning-tree mst configuration FS(config-mst)# instance 1 vlan 100, 1-99, 101-2000 FS(config-mst)# exit FS(config)# erps raps-vlan 100 FS(config-erps100)#protected-instance 1 # Configure the VLAN configured by the ERP2. FS(config)# spanning-tree mst configuration FS(config-mst)# instance 2 vlan 4093, 2001-4092, 4094 FS(config-mst)# exit FS(config)# erps raps-vlan 4093 FS(config-erps4093)#protected-instance 2</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.6 ring-port

	Use this command to configure the ERPS ring.	
	ring-port west { <i>interface-name1</i> virtual-channel } east { <i>interface-name2</i> virtual-channel }	
	no ring-port	
Parameter Description	Parameter	Description
	<i>interface-name1</i>	Name of the West port.
	<i>interface-name2</i>	Name of the East port.
Defaults	No ERPS ring is configured.	
Command Mode	ERPS configuration mode.	
Usage Guide	1) After adding the port to the ERP ring, the trunk attribute of the port is not allowed to be modified any more. 2) If the ring port is configured on the virtual-channel, this ring will be considered as a sub-ring. 3) Ports running the ERPS do not participate in the STP computing. ERPS, RERP and REUP do not share the port.	
Configuration Examples	The following example is for the ERPS ring. <pre># Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Configure the link mode of the Ethernet ring port and the default VLAN. FS(config)# interface fastEthernet 0/1 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# interface fastEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# exit # Enter the ERPS configuration mode. FS(config)# erps raps-vlan 4093 #Add the ports that participate in the ERPS protocol computing to the Ethernet ring. FS(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2</pre>	
Related Commands	Command	Description
	state enable	Enable the ERPS protocol of the specified ring in the ERPS mode of the specified ring.

	sub-ring associate raps-vlan <i>vlan-id</i>	Establish the association between the subring and other Ethernet rings in the subring ERPS configuration mode.
Platform Description	N/A	

11.7 rpl-port

	Use this command to configure the RPL port and RPL owner.	
	rpl-port { <i>west</i> <i>east</i> } [rpl-owner]	
	no rpl-port	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No RPL port and RPL owner are configured.	
Command Mode	ERPS configuration mode.	
Usage Guide	Up to one RPL link and one RPL owner node are needed and configurable for each ring.	
Configuration Examples	The following example configures the RPL port and RPL owner. <pre># Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Configure the link mode of the Ethernet ring port and the default VLAN. FS(config)# interface fastEthernet 0/1 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# interface fastEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# exit # Enter the ERPS configuration mode. FS(config)# erps raps-vlan 4093 # Add the ports that participate in the ERPS protocol computing to the Ethernet ring. FS(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2 # Specify the port where the RPL link is and the RPL owner.</pre>	

	FS(config-erps4093)# rpl-port west rpl-owner	
Related Commands	Command	Description
	ring-port west { <i>interface-name1</i> virtual-channel } east { <i>interface-name2</i> virtual-channel }	Configure the specified ERP ring in the ERPS configuration mode of the specified ring.
	state enable	Enable the ERPS protocol of the specified ring in the ERPS configuration mode of the specified ring.
Platform Description	N/A	

11.8 show erps

	Use this command to show the parameters and states of the ERPS.	
	show erps [{ global raps_vlan <i>vlan-id</i> [sub-ring]]	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example shows the use of this command. <pre> FS# show erps ERPS Information Global Status : Enabled Link monitored by : Not Oam ----- R-APS VLAN : 4092 Ring Status : Enabled West Port : Gi 0/5 (Blocking) East Port : Gi 0/7 (Forwarding) RPL Port : West Port RPL Port Blocked VLAN : All RPL Owner : Enabled Holdoff Time : 0 milliseconds Guard Time : 500 milliseconds WTR Time : 5 minutes </pre>	

<pre> Current Ring State : Idle ----- R-APS VLAN : 4093 Ring Status : Enabled West Port : Virtual Channel East Port : Gi 0/10 (Forwarding) RPL Port : None RPL Port Blocked VLAN : All RPL Owner : Disabled Holdoff Time : 0 milliseconds Guard Time : 500 milliseconds WTR Time : 5 minutes Current Ring State : Idle ----- R-APS VLAN : 4094 Ring Status : Enabled West Port : Virtual Channel East Port : 12 (Forwarding) RPL Port : None RPL Port Blocked VLAN : All RPL Owner : Disabled Holdoff Time : 0 milliseconds Guard Time : 500 milliseconds WTR Time : 5 minutes Current Ring State : Idle FS# show erps raps_vlan 4093 sub-ring R-APS VLAN: 4093 Sub-Ring R-APS VLANs TC Propagation State ----- 100 Enable 200 Enable </pre>		
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.9 state enable

	Use this command to enable/disable the specified R-APS ring.	
	state enable	
	no state enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Disabled	
Command Mode	EPRS configuration mode.	
Usage Guide	Only after the global ERPS protocol and the ERPS protocol of the specified ring are both enabled, the ERPS protocol of the specified ring will begin truly running.	
Configuration Examples	The following example enables the specified ERPS ring: <pre>#Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. #Configure the link mode of the Ethernet ring port and the default VLAN. FS(config)# interface fastEthernet 0/1 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# interface fastEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# exit # Enter the ERPS configuration mode. FS(config)# erps raps-vlan 4093 # Add the ports that participate in the ERPS protocol computing to the Ethernet ring. FS(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2 # Enable the ERPS function for the specified ring. FS(config-erps4093)#state enable # Enable the global ERPS function. FS(config-erps4093)# exit FS(config)# erps enable</pre>	

Related Commands	Command	Description
	erps enable	Enable the global ERPS protocol.
Platform Description	N/A	

11.10 sub-ring tc-propagation

	Use this command to specify the devices corresponding to the crossing node on the crossing ring whether to send out the notification when the subring topology changes.	
	sub-ring tc_propagation enable	
	no sub-ring tc_propagation	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the topology changing notification is not sent.	
Command Mode	EPRS configuration mode.	
Usage Guide	This command is just needed to be configured on the crossing nodes on the crossing ring.	
Configuration Examples	The following example is configured when the subring topology changes. <pre># Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. #Configure the link mode of the Ethernet ring port and the default VLAN. FS(config)# interface fastEthernet 0/1 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# interface fastEthernet 0/2 FS(config-if)# switchport mode trunk FS(config-if)# exit # Enter the ERPS configuration mode. FS(config)# erps raps-vlan 4093 # Add the ports that participate in the ERPS protocol computing to the Ethernet ring. FS(config-erps4093)# ring-port west fastEthernet 0/1 east fastEthernet 0/2</pre>	

	<pre>#Configure the Ethernet subring. FS(config)# erps raps-vlan 100 FS(config)# interface fastEthernet 0/3 FS(config-if)# switchport mode trunk FS(config-if)# exit FS(config)# erps raps-vlan 100 FS(config-erps100)# ring-port west fastEthernet 0/3 east virtual-channel # Associate the subring with other Ethernet rings. FS(config-erps100)# sub-ring associate raps-vlan 4093 # Enable the topology changing notification for the subring. FS(config-erps100)# sub-ring tc-propagation enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.11 timer

	Use this command to configure the timer of the ERPS protocol.	
	timer { holdoff-time interval1 guard-time interval2 wtr-time interval3 }	
	no timer { holdoff-time guard-time wtr-time }	
Parameter Description	Parameter	Description
	interval1	Value of the Holdoff timer in 100 milliseconds, the valid range is 0 to 100.
	Interval2	Value of the Guard timer in 10 milliseconds, the valid range is 1 to 200.
	Interval3	Value of the WTR in minute, the valid range is 5 to 12.
Defaults	Holdoff timer: 0. Guard timer: 500 milliseconds. WTP timer: 5 seconds.	
Command Mode	ERPS configuration mode.	
Usage Guide	Holdoff timer: This timer is used to avoid the ERPS from topology switchingswitching continuously due to the link intermittent fault. With this timer configured, if the link fault is detected, the ERPS does not perform the topology switching immediately until the timer times out and the link fault is verified. Guard timer: This timer is used to prevent the device receiving the timed-out R-APS messages. When the device	

	detects the recovery from failure of the link, it sends out the message of link recovery and starts up the Guard timer. Before the Guard times out, except for the flush packets indicating the subring topology change, other packets are discarded directly without being handled.	
	WTR (Wait-to-restore) timer: This timer is only valid for the RPL owner device. It is mainly used to prevent the RPL owner making the erroneous judgment to the ring network status. When the RPL detects the fault recovery, it does not perform the topology switching immediately until the WTR times out and the Ethernet ring indeed recovers from the fault. If the ring network fault is checked again before the WTR times out, then the WTR timer will be canceled and topology switching will be not executed any longer.	
Configuration Examples	The following example configures the timer of the ERPS protocol. # Enter the privileged EXEC mode. FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. # Enter the ERPS configuration mode. FS(config)# erps raps-vlan 4093 # Configure the protocol timer. FS(config-erps4093)# timer holdoff-time 10 FS(config-erps4093)# timer guard-time 10 FS(config-erps4093)# timer wtr-time 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

IP Address & Application Commands

11 IP Address/Service Commands

1.1 gateway

	Use this command to set the gateway address for the management port. Use the no form of this command to remove the setting.	
	gateway address	
	no gateway	
Parameter	Parameter	Description
Description	address	Sets the gateway address for the management port
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the gateway address for the management port to 1.1.1.1. <pre>FS(config)# interface mgmt 0 FS(config-if-Mgmt 0)# gateway 1.1.1.1 FS(config-if-Mgmt 0)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.2 ip-address

	Use this command to configure the IP address of an interface. Use the no form of this command to restore the default setting.	
	ip address <i>ip-address network-mask</i> [secondary]	
	no ip address [<i>ip-address network-mask</i> [secondary]	
Parameter	Parameter	Description
Description	ip-address	32-bit IP address, with 8 bits in one group in decimal format. Groups are separated by dots.
	network-mask	32-bit network mask. 1 stands for the mask bit, 0 stands for the host bit, with 8 bits in one group in decimal format. Groups are separated by dots.

	secondary	Secondary IP address				
Defaults	No IP address is configured for the interface by default.					
Command Mode	Interface configuration mode					
Usage Guide	The equipment cannot receive and send IP packets before it is configured with an IP address. After an IP address is configured for the interface, the interface is allowed to run the Internet Protocol (IP). The network mask is also a 32-bit value that identifies which bits among the IP address is the network portion. Among the network mask, the IP address bits that correspond to value “1” are the network address. The IP address bits that correspond to value “0” are the host address. For example, the network mask of Class A IP address is “255.0.0.0”. You can divide a network into different subnets using the network mask. Subnet division means to use the bits in the host address part as the network address part, so as to reduce the capacity of a host and increase the number of networks. In this case, the network mask is called subnet mask. The FSOS software supports multiple IP address for an interface, in which one is the primary IP address and others are the secondary IP addresses. Theoretically, there is no limit for the number of secondary IP addresses. The primary IP address must be configured before the secondary IP addresses. The secondary IP address and the primary IP address must belong to the same network or different networks. Secondary IP addresses are often used in network construction. Typically, you can try to use secondary IP addresses in the following situations: A network hasn’t enough host addresses. At present, the LAN should be a class C network where 254 hosts can be configured. However, when there are more than 254 hosts in the LAN, another class C network address is necessary since one class C network is not enough. Therefore, the device should be connected to two networks and multiple IP addresses should be configured. Many older networks are layer 2-based bridge networks that have not been divided into different subnets. Use of secondary IP addresses will make it very easy to upgrade this network to an IP layer-based routing network. The equipment configures an IP address for each subnet. Two subnets of a network are separated by another network. You can create a subnet for the separated network, and connect the separated subnet by configuring a secondary IP address. One subnet cannot appear on two or more interfaces of a device.					
Configuration Examples	The following example configures the primary IP address and the network mask as 10.10.10.1 and 255.255.255.0 respectively . <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip interface</td><td>Displays detailed information of the interface.</td></tr></table>	Command	Description	show ip interface	Displays detailed information of the interface.	
Command	Description					
show ip interface	Displays detailed information of the interface.					

Platform	N/A
Description	

1.3 ip address-pool local

	Use this command to enable the IP address pool function. Use the no form of this command to disable this function.	
	ip address-pool local	
	no ip address-pool local	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This function is enabled by default. PPP users can allocate an IP address to the peer end from the IP address pool configured. If you can use the no ip address-pool local command to disable this function and clear all configured IP address pools.	
Configuration Examples	The following example enables the IP address pool function. FS(config)# ip address-pool local	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

1.4 ip broadcast-addresss

	Use this command to define a broadcast address for an interface in the interface configuration mode. Use the no form of this command to restore the default setting.	
	ip broadcast-addresss <i>ip-address</i>	
	no ip broadcast-addresss	
Parameter	Parameter	Description
Description	<i>ip-address</i>	Broadcast address of IP network
Defaults	The default IP broadcast address is 255.255.255.255.	
Command Mode	Interface configuration mode.	

Usage Guide	At present, the destination address of IP broadcast packet is all “1”, represented as 255.255.255.255. The FSOS software can generate broadcast packets with other IP addresses through definition, and can receive both all “1” and the broadcast packets defined by itself.	
Configuration Examples	The following example sets he destination address of IP broadcast packets generated by this interface to 0.0.0.0. FS(config)# interface gigabitEthernet 0/1 FS(config-if)# ip broadcast-address 0.0.0.0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.5 ip icmp error-interval

	Use this command to set the rate to send the ICMP destination unreachable packets triggered by DF in the IP header. Use the no form of this command to restore the default setting.	
	ip icmp error-interval DF milliseconds [<i>bucket-size</i>]	
	no ip icmp error-interval DF milliseconds [<i>bucket-size</i>]	
	Use this command to set the rate to send other ICMP error packets. Use the no form of this command to restore the default setting.	
	ip icmp error-interval milliseconds [bucket-size]	
	no ip icmp error-interval milliseconds [<i>bucket-siz</i>]	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	The refresh period of the token bucket, in the range from 0 to 2147483647 in the unit of milliseconds. 0 indicates no limit on the rate to send ICMP error packets. The default is 100.
	<i>bucket-size</i>	The number of tokens in the bucket, in the range is from 1 to 200. The default is 10.
Defaults	The default rate is 10 packets per 100 millisecond.	
Command Mode	Global configuration mode.	
Usage Guide	To prevent DoS attack, the token bucket algorithm is adopted to limit the rate to send ICMP error packets. If IP packets need to be fragmented while the DF is set to 1, the device sends ICMP destination unreachable packets numbered 4 to the source IP address for path MTU discovery. Rate limits on ICMP destination unreachable packets and other error packets are needed to prevent path MTU discovery failure.	

	It is recommended to set the refresh period to an integral multiple of 10 milliseconds. If the refresh period is not an integral multiple of 10 milliseconds, it is adjusted automatically. For example, 1 per 5 milliseconds is adjusted to 2 per 10 milliseconds; 3 per 15 milliseconds is adjusted to 2 per 10 milliseconds.	
Configuration Examples	The following example sets the rate to send the ICMP destination unreachable packets triggered by DF in the IP header to 100 per second. <pre>FS(config)# ip icmp error-interval DF 1000 100</pre> The following example sets the rate to send other ICMP error packets to 10 per second. <pre>FS(config)# ip icmp error-interval 1000 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.6 ip icmp timestamp

	Use this command to enable the device to return a Timestamp Reply. Use the no form of this command to disable returning of Timestamp Reply.	
	ip icmp timestamp	
	no ip icmp timestamp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example disables the device to return a Timestamp Reply. <pre>FS(config)# no ip icmp timestamp</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.7 ip directed-broadcast

	Use this command to enable the conversion from IP directed broadcast to physical broadcast in the interface configuration mode. Use the no form of this command to restore the default setting.	
	ip directed-broadcast [<i>access-list-number</i>]	
	no ip directed-broadcast	
Parameter Description	Parameter	Description
	<i>access-list-number</i>	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet. The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in the manner of link layer broadcast. You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets. You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast. If the no ip directed-broadcast command is configured on an interface, FSOS will discard the directed broadcast packets received from the directly connected network.	
Configuration Examples	The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 port of a device. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# ip directed-broadcast</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.8 ip local pool

	Use this command to create an IP address pool. Use the no form of this command to remove the setting.	
	ip local pool <i>pool-name</i> <i>low-ip-address</i> [<i>high-ip-address</i>]	
	no ip local pool <i>pool-name</i> [<i>low-ip-address</i> [<i>high-ip-address</i>]]	
Parameter	Parameter	Description
Description	<i>pool-name</i>	Specifies the address pool name. The default name is default .
	<i>low-ip-address</i>	The start IP address in the address pool.
	<i>high-ip-address</i>	(Optional) The end IP address in the address pool.
Defaults	No IP address pool is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to create one or multiple IP address pools for PPP to allocate addresses to users.	
Configuration Examples	The following example creates an IP address pool named quark ranging from 172.16.23.0 to 172.16.23.255. FS(config)#ip local pool quark 172.16.23.0 172.16.23.255	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.9 ip mask-reply

	Use this command to configure the FSOS software to respond the ICMP mask request and send an ICMP response message in the interface configuration mode. Use the no form of this command to restore the default setting.	
	ip mask-reply	
	no ip mask-reply	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	

Command mode	Interface configuration mode.	
Usage Guide	Sometimes, a network device needs the subnet mask of a subnet on the Internet. To obtain such information, the network device can send an ICMP mask request message, and the network device that receives this message will send a mask response message.	
Configuration Examples	The following example sets the FastEthernet 0/1 interface of a device to respond the ICMP mask request message. FS(config)# interface fastEthernet 0/1 FS(config-if)# ip mask-reply	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.10 ip mtu

	Use this command to set the Maximum Transmission Unit (MTU) for an IP packet in the interface configuration mode. Use the no form of this command is restore the default setting.	
	ip mtu bytes	
	no ip mtu	
Parameter	Parameter	Description
Description	bytes	Maximum transmission unit of IP packet , in the range from 68 to 1500 bytes
Defaults	It is the same as the value configured in the interface command mtu by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If an IP packet is larger than the IP MTU, the FSOS software will split this packet. All the devices in the same physical network segment must have the same IP MTU for the interconnected interface. If the interface configuration command mtu is used to set the maximum transmission unit value of the interface, IP MTU will automatically match with the MTU value of the interface. However, if the IP MTU value is changed, the MTU value of the interface will remain unchanged.	
Configuration Examples	The following iexample sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# ip mtu 512</pre>	
Related Commands	Command	Description
	mtu	Sets the MTU value of an interface.

Platform Description	N/A

1.11 ip redirects

	Use this command to allow the FSOS software to send an ICMP redirection message in the interface configuration mode. Use the no form of this command to disable this function.	
	ip redirects	
	no ip redirects	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	When the route is not optimum, it may make the device to receive packets through one interface and send it though the same interface. If the device sends the packet through the interface through which this packet is received, the device will send an ICMP redirection message to the data source, telling the data source that the gateway for the destination address is another device in the subnet. In this way the data source will send subsequent packets along the optimum path.	
Configuration Examples	The following example disables ICMP redirection for the fastEthernet 0/1 interface. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# no ip redirects</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.12 ip source-route

	Use this command to allow the FSOS software to process an IP packet with source route information in global configuration mode. Use the no form of this command to disable this function.	
	ip source-route	
	no ip source-route	
Parameter	Parameter	Description
Description	N/A	N/A

Defaults	This function is enabled by default.					
Command Mode	Global configuration mode.					
Usage Guide	FSOS supports IP source route. When the device receives an IP packet, it will check the options of the IP packet, such as strict source route, loose source route and record route. Details about these options can be found in RFC 791. If an option is found to be enabled in this packet, a response will be made. If an invalid option is detected, an ICMP parameter problem message will be sent to the data source, and then this packet is discarded.					
Configuration Examples	The following example disables the IP source route. FS(config)# no ip source-route					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

1.13 ip ttl

	Use this command to set the TTL value of the unicast packet. Use the no form of this command to restore the default setting.	
	ip ttl <i>value</i>	
	no ip ttl	
Parameter	Parameter	Description
Description	<i>value</i>	Sets the TTL value of the unicast packet, in the range from 0 to 255.
Defaults	The default is 64.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the TTL value of the unicast packet to 100. FS(config)# ip ttl 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.14 ip ttl-expires enable

	This command is used to enable notifications of expired TTL. Use the no form of this command to disable this function.	
	ip ttl-expires enable	
	no ttl-expires enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, notifications are enabled to indicate expired TTL.	
Command mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example disables notifications indicating expired TTL. <pre>FS(config)# no ttl-expires enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.15 ip unnumbered

	This command is used to configure unnumbered interfaces. After an interface is set to an unnumbered interface, IP can be run on the interface and packets can be sent or received on the interface. Use the no form of this command to restore the default setting.	
	ip unnumbered <i>interface-type interface-number</i>	
	no ip unnumbered	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Type of the associated interface
	<i>interface-number</i>	No. of the associated interface

Defaults	No unnumbered interface is configured by default.				
Command mode	Interface configuration mode				
Usage Guide	An unnumbered interface indicates that IP is enabled on the interface but no IP address is allocated for the interface. An unnumbered interface must associate with an interface with an IP address. The source IP address of the IP packets generated on an unnumbered interface is the IP address of the associated interface. In addition, the routing protocol process determines whether to send route update packets to the unnumbered interface according to the IP address of the associated interface. Pay attention to the following when using an unnumbered interface: An Ethernet interface cannot be set to an unnumbered interface. When SLIP, HDLC, PPP, LAPB, and Frame-relay are encapsulated on a serial port, the port can be set to an unnumbered interface. When a frame relay is encapsulated, only a point-to-point subinterface can be set to an unnumbered interface. In the case of X.25 encapsulation, unnumbered interface is not allowed. The ping command cannot be used to check whether an unnumbered interface is working properly because the interface does not have an IP address. The status of an unnumbered interface can be remotely monitored over SNMP. The network cannot be enabled using an unnumbered interface.				
Configuration Examples	The following example configures the local interface as an unnumbered interface and sets the associated interface to FastEthernet 0/1 (an IP address is configured for the interface). <pre>FS(config-if)# ip unnumbered fastEthernet 0/1</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show interface</td><td>Displays the detailed information about the interface.</td></tr> </table>	Command	Description	show interface	Displays the detailed information about the interface.
Command	Description				
show interface	Displays the detailed information about the interface.				
Platform Description	N/A				

1.16 ip unreachable

	Use this command to allow the FSOS software to generate ICMP destination unreachable messages. Use the no form of this command to disable this function.	
	ip unreachable	
	no ip unreachable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	

Command Mode	Interface configuration mode.				
Usage Guide	FSOS software will send a ICMP destination unreachable message if it receives unicast message with self-destination-address and can not process the upper protocol of this message. FSOS software will send ICMP host unreachable message to source data if it can not forward a message due to no routing. This command influences all ICMP destination unreachable messages.				
Configuration Examples	The following example disables sending ICMP destination unreachable message on FastEthernet 0/1. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# no ip unreachable</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

1.17 show ip interface

	Use this command to display the IP status information of an interface.	
	show ip interface [<i>interface-type interface-number</i> brief]	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Specifies interface type.
	<i>interface-number</i>	Specifies interface number.
	<i>brief</i>	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	When an interface is available, FSOS will create a direct route in the routing table. The interface is available in that the FSOS software can receive and send packets through this interface. If the interface changes from available status to unavailable status, the FSOS software removes the appropriate direct route from the routing table. If the interface is unavailable, for example, two-way communication is allowed, the line protocol status will be shown as "UP". If only the physical line is available, the interface status will be shown as "UP".	

The results shown may vary with the interface type, because some contents are the interface-specific options

Configuration

Examples

The following example displays the output of the **show ip interface brief** command.

```
FS#show ip interface brief
```

```
Interface IP-Address(Pri) IP-Address(Sec) Status Protocol
```

```
GigabitEthernet 0/10 2.2.2.2/24 3.3.3.3/24 down down
```

```
GigabitEthernet 0/11 no address no address down down
```

```
VLAN 1 1.1.1.1/24 no address down down
```

Description of fields:

Field	Description
Status	Link status of an interface. The value can be up , down , or administratively down .
Protocol	IPv4 protocol status of an interface.

The following example displays the output of the **show ip interface vlan** command.

```
SwitchA#show ip interface vlan 1
```

```
VLAN 1
```

```
IP interface state is: DOWN
```

```
IP interface type is: BROADCAST
```

```
IP interface MTU is: 1500
```

```
IP address is:
```

```
1.1.1.1/24 (primary)
```

```
IP address negotiate is: OFF
```

```
Forward direct-broadcast is: OFF
```

```
ICMP mask reply is: ON
```

```
Send ICMP redirect is: ON
```

```
Send ICMP unreachable is: ON
```

```
DHCP relay is: OFF
```

```
Fast switch is: ON
```

```
Help address is:
```

```
Proxy ARP is: OFF
```

```
ARP packet input number: 0
```

```
Request packet: 0
```

```
Reply packet: 0
```

```
Unknown packet: 0
```

```
TTL invalid packet number: 0
```

```
ICMP packet input number: 0
```

```
Echo request: 0
```

```
Echo reply: 0
```

```
Unreachable: 0
```

```
Source quench: 0
```

```
Routing redirect: 0
```

Description of fields in the results:

Field	Description
IP interface state is:	The network interface is available, and both its interface hardware status and line protocol status are "UP".
IP interface type is:	Show the interface type, such as broadcast, point-to-point, etc.
IP interface MTU is:	Show the MTU value of the interface.
IP address is:	Show the IP address and mask of the interface.
IP address negotiate is:	Show whether the IP address is obtained through negotiation.
Forward direct-broadcast is:	Show whether the directed broadcast is forwarded.
ICMP mask reply is:	Show whether an ICMP mask response message is sent.
Send ICMP redirect is:	Show whether an ICMP redirection message is sent.
Send ICMP unreachable is:	Show whether an ICMP unreachable message is sent.
DHCP relay is:	Show whether the DHCP relay is enabled.
Fast switch is:	Show whether the IP fast switching function is enabled.
Route horizontal-split is:	Show whether horizontal split is enabled, which will affect the route update behavior of the distance vector protocol.
Help address is:	Show the helper IP address.
Proxy ARP is:	Show whether the agent ARP is enabled.
ARP packet input number: Request packet: Reply packet: Unknown packet:	Show the total number of ARP packets received on the interface, including: ARP request packet ARP reply packet Unknown packet
TTL invalid packet number:	Show the TTL invalid packet number
ICMP packet input number: Echo request: Echo reply: Unreachable: Source quench: Routing redirect:	Show the total number of ICMP packets received on the interface, including: Echo request packet Echo reply packet Unreachable packet Source quench packet Routing redirection packet
Outgoing access list is	Show whether an outgoing access list has been configured for an interface.
Inbound access list is	Show whether an incoming access list has been configured for an interface.

**Related
Commands**

Command	Description
N/A.	N/A.

Platform	N/A.
Description	

1.18 show ip packet queue

	Use this command to display the statistics of IP packet queues.									
	show ip packet queue									
Parameter	Parameter	Description								
Description	N/A	N/A								
Defaults	N/A									
Command Mode	Privileged EXEC mode.									
Usage Guide	N/A.									
Configuration Examples	The following example displays the statistics of IP packet queues. <pre>FS#show ip packet queue Receive 31925 packets(fragment=0): IP packet receive queue: length 0, max 1542, overflow 0. Receive 13 ICMP echo packets, 25 ICMP reply packets . Discards: Failed to alloc skb: 0. Receive queue overflow: 0. Unknow protocol drops: 0. ICMP rcv drops: 0. for skb check fail. ICMP rcv drops: 0. for skb is broadcast. Sent packets: Success: 15644 Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets. It records 187 us as max time in ICMP reply process. Failed to alloc ebuf: 0 Dropped by EFMP: 0 NoRoutes: 887 Get vrf fails: 0 Cannot assigned address drops: 0 Failed to encapsulate ethernet head: 0 ICMP error queue: length 0, max 1542, overflow 0.</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>IP packet receive queue</td><td>Statistics of received packets</td></tr><tr><td>Discards</td><td>Statistics of discarded packets</td></tr><tr><td>Sent packets</td><td>Statistics of sent packets</td></tr></table>		Field	Description	IP packet receive queue	Statistics of received packets	Discards	Statistics of discarded packets	Sent packets	Statistics of sent packets
Field	Description									
IP packet receive queue	Statistics of received packets									
Discards	Statistics of discarded packets									
Sent packets	Statistics of sent packets									

	ICMP error queue	Statistics of ICMP error packets
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

1.19 show ip packet statistics

	Use this command to display the statistics of IP packets.	
	show ip packet statistics [total interface-name]	
Parameter	Parameter	Description
Description	interface-name	Interface name
	total	Displays the total statistics of all interfaces.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A.	
Configuration	The following example displays the output of this command.	
Examples	<pre> FS# show ip packet statistics Total Received 1000 packets, 1000000 bytes Unicast:1000,Multicast:0,Broadcast:0 Discards:0 HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0) NoRoutes:0 Others:0 Sent 100 packets, 6000 bytes Unicast:50,Multicast:50,Broadcast:0 VLAN 1 Received 1000 packets, 1000000 bytes Unicast:1000,Multicast:0,Broadcast:0 Discards:0 HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0) NoRoutes:0 Others:0 Sent 100 packets, 6000 bytes Unicast:50,Multicast:50,Broadcast:0 </pre>	

Related Commands	Command	Description
	ip default-gateway	Configures the default gateway, which is only supported on the Layer 2 switch.
Platform	N/A	
Description		

1.20 show ip pool

	Use this command to display the IP address pool.			
	show ip pool [<i>pool-name</i>]			
Parameter Description	Parameter	Description		
	<i>pool-name</i>	Specifies the IP address pool.		
Defaults	N/A			
Command Mode	Privileged EXEC mode			
Usage Guide	N/A			
Configuration Examples	The following example displays all IP address ranges.			
	FS# show ip pool			
	FS(config)#show ip pool			
	Pool	Begin	End	Free In use
	default	1.1.1.1	1.1.1.1	1 0
	pool1	2.2.2.2	2.2.2.254	253 0
	pool2	3.1.1.1	3.2.1.1	65537 0
	pool3	192.168.1.1	192.168.1.254	
	Field		Description	
	Pool		Address pool name	
	Begin		The start IP address of the address pool	
	Free		The number of free IP addresses in the address pool	
In use		The number of IP addresses in use in the address pool		
Related Commands	Command	Description		
	N/A	N/A		
Platform Description	N/A			

1.21 show ip raw-socket

	Use this command to display IPv4 raw sockets.	
	show ip raw-socket [<i>num</i>]	
Parameter	Parameter	Description
Description	<i>num</i>	Protocol.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A.	
Configuration	The following example displays all IPv4 raw sockets.	
Examples	FS# show ip raw-socket	
	Number Protocol Process name	
	1	ICMP dhcp.elf
	2	ICMP vrrp.elf
	3	IGMP igmp.elf
	4	VRRP vrrp.elf
	Total: 4	
	Field Description	
	Field	Description
	Number	Number
	Protocol	Protocol
	Process name	Process name
	Total	Total number
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

1.22 show ip sockets

	Use this command to display all IPv4 sockets.	
	show ip sockets	
Parameter	Parameter	Description
Description	N/A.	N/A.

Defaults	N/A.						
Command Mode	Privileged EXEC mode.						
Usage Guide	N/A.						
Configuration	The following displays all IPv4 sockets.						
Examples	FS# show ip sockets						
	Number	Process name	Type	Protocol	LocalIP:Port	ForeignIP:Port	State
	1	dhcp.elf	RAW	ICMP	0.0.0.0:1	0.0.0.0:0	*
	2	vrrp.elf	RAW	ICMP	0.0.0.0:1	0.0.0.0:0	*
	3	igmp.elf	RAW	IGMP	0.0.0.0:2	0.0.0.0:0	*
	4	vrrp.elf	RAW	VRRP	0.0.0.0:112	0.0.0.0:0	*
	5	dhcpc.elf	DGRAM	UDP	0.0.0.0:68	0.0.0.0:0	*
	6	snmpd	DGRAM	UDP	0.0.0.0:161	0.0.0.0:0	*
	7	wbav2	DGRAM	UDP	0.0.0.0:2000	0.0.0.0:0	*
	8	vrrp_plus.elf	DGRAM	UDP	0.0.0.0:3333	0.0.0.0:0	*
	9	mpls.elf	DGRAM	UDP	0.0.0.0:3503	0.0.0.0:0	*
	10	rds_other_th	DGRAM	UDP	0.0.0.0:3799	0.0.0.0:0	*
	11	snmpd	DGRAM	UDP	0.0.0.0:14800	0.0.0.0:0	*
	12	sshd	STREAM	TCP	0.0.0.0:22	0.0.0.0:0	LISTEN
	13	telnetd	STREAM	TCP	0.0.0.0:23	0.0.0.0:0	LISTEN
	14	wbard	STREAM	TCP	0.0.0.0:4389	0.0.0.0:0	LISTEN
	15	wbard	STREAM	TCP	0.0.0.0:7165	0.0.0.0:0	LISTEN
Total: 15							
Field Description							
Field			Description				
Number			Serial number.				
Process name			Process name.				
Type			Socket type, including the following types: RAW: raw sockets DGRAM: datagram type STREAM: stream type.				
Protocol			Protocol.				
LocalIP:Port			Local IP address and port.				
ForeignIP:Port			Peer IP address and port.				
State			State. This field is for only TCP sockets.				
Total			The total number of sockets.				
Related Commands	Command			Description			
	N/A			N/A			
Platform	N/A						
Description							

1.23 show ip udp

	Use this command to display IPv4 UDP sockets.																																												
	show ip udp [local-port <i>num</i>]																																												
	Use this command to display IPv4 UDP socket statistics.																																												
	show ip udp statistics																																												
Parameter	Parameter	Description																																											
Description	local-port <i>num</i>	Local port number																																											
Defaults	N/A.																																												
Command Mode	Privileged EXEC mode.																																												
Usage Guide	N/A.																																												
Configuration Examples	The following example displays all IPv4 UDP sockets. <pre>FS# show ip udp</pre> <table><tr><th>Number</th><th>Local Address</th><th>Peer Address</th><th>Process name</th></tr><tr><td>1</td><td>0.0.0.0:68</td><td>0.0.0.0:0</td><td>dhcpc.elf</td></tr><tr><td>2</td><td>0.0.0.0:161</td><td>0.0.0.0:0</td><td>snmpd</td></tr><tr><td>3</td><td>0.0.0.0:2000</td><td>0.0.0.0:0</td><td>wbav2</td></tr><tr><td>4</td><td>0.0.0.0:3333</td><td>0.0.0.0:0</td><td>vrrp_plus.elf</td></tr><tr><td>5</td><td>0.0.0.0:3503</td><td>0.0.0.0:0</td><td>mpls.elf</td></tr><tr><td>6</td><td>0.0.0.0:3799</td><td>0.0.0.0:0</td><td>rds_other_th</td></tr><tr><td>7</td><td>0.0.0.0:14800</td><td>0.0.0.0:0</td><td>snmpd</td></tr></table> Field Description <table><tr><th>Field</th><th>Description</th></tr><tr><td>Number</td><td>Number.</td></tr><tr><td>Local Address</td><td>Local IP address and port.</td></tr><tr><td>Peer Address</td><td>Peer IP address and port.</td></tr><tr><td>Process name</td><td>Process name.</td></tr></table>			Number	Local Address	Peer Address	Process name	1	0.0.0.0:68	0.0.0.0:0	dhcpc.elf	2	0.0.0.0:161	0.0.0.0:0	snmpd	3	0.0.0.0:2000	0.0.0.0:0	wbav2	4	0.0.0.0:3333	0.0.0.0:0	vrrp_plus.elf	5	0.0.0.0:3503	0.0.0.0:0	mpls.elf	6	0.0.0.0:3799	0.0.0.0:0	rds_other_th	7	0.0.0.0:14800	0.0.0.0:0	snmpd	Field	Description	Number	Number.	Local Address	Local IP address and port.	Peer Address	Peer IP address and port.	Process name	Process name.
Number	Local Address	Peer Address	Process name																																										
1	0.0.0.0:68	0.0.0.0:0	dhcpc.elf																																										
2	0.0.0.0:161	0.0.0.0:0	snmpd																																										
3	0.0.0.0:2000	0.0.0.0:0	wbav2																																										
4	0.0.0.0:3333	0.0.0.0:0	vrrp_plus.elf																																										
5	0.0.0.0:3503	0.0.0.0:0	mpls.elf																																										
6	0.0.0.0:3799	0.0.0.0:0	rds_other_th																																										
7	0.0.0.0:14800	0.0.0.0:0	snmpd																																										
Field	Description																																												
Number	Number.																																												
Local Address	Local IP address and port.																																												
Peer Address	Peer IP address and port.																																												
Process name	Process name.																																												
Related Commands	Command	Description																																											
	N/A	N/A																																											
Platform Description	N/A																																												

2 ARP Commands

2.1 arp

	Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use the no form of this command to restore the default setting.	
	arp [vrf name] <i>ip-address</i> <i>MAC-address</i> <i>type</i>	
	no arp [vrf name] <i>ip-address</i>	
Parameter	Parameter	Description
Description	vrf name	VRF instance. Set the <i>name</i> parameter to configure a name for the VRF instance. By default, no VRF instance is specified. The configured static ARP is global.
	ip-address	The IP address that corresponds to the MAC address. It includes four parts of numeric values in decimal format separated by dots.
	MAC-address	48-bit data link layer address
	type	ARP encapsulation type. The keyword is arpa for the Ethernet interface.
Defaults	There is no static mapping record in the ARP cache table by default.	
Command Mode	Global configuration mode.	
Usage Guide	FSOS finds the 48-bit MAC address according to the 32-bit IP address using the ARP cache table. Since most hosts support dynamic ARP resolution, usually static ARP mapping is not necessary. The clear arp-cache command can be used to delete the ARP mapping that is learned dynamically.	
Configuration Examples	The following example sets an ARP static mapping record for a host in the Ethernet. FS(config)# arp 1.1.1.1 4e54.3800.0002 arpa	
Related Commands	Command	Description
	clear arp-cache	Clears the ARP cache table
Platform Description	N/A	

2.2 arp-learning

	Use this command to enable ARP learning. Use the no form of this command to disable this function.	
	arp-learning enable	
	no arp-learning enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default	

Command Mode	Interface configuration mode					
Usage Guide	After the device learns the dynamic ARP and turns it to the static ARP through Web, it is recommended to enable ARP learning. Otherwise, it is not recommended to enable this function. If this function is disabled with dynamic ARP existing, you can turn dynamic ARP to static ARP through Web. You can also clear the dynamic ARP using the clear arp command to deny the specified user's access to Internet. Otherwise, the dynamic ARP will be aged and then cleared. After this function is disabled, the AnyIP function and trust ARP detection are disabled.					
Configuration Examples	The following example enables ARP learning. <pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# arp-learning enable</pre> The following example disables ARP learning. <pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# no arp-learning enable</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

2.3 arp anti-ip-attack

	Use this command to configure ARP anti-ip-attack. Use the no form of this command to restore the default setting.	
	arp anti-ip-attack <i>num</i>	
	no arp anti-ip-attack	
Parameter	Parameter	Description
Description	<i>num</i>	The number of the IP message to trigger the ARP to discarded entry in the range from 0 to 100. 0 stands for disabling the arp anti-ip-attack function.
Defaults	By default, set the discarded entry after 3 unknown unicast messages are sent to the CPU.	
Command Mode	Global configuration mode.	
Usage Guide	For the messages corresponds to the directly-connected route, if the switch does not learn the ARP that corresponds to the destination IP address, it is not able to forward the message in hardware, and it needs to send the message to the CPU to resolve the address(that is the ARP learning). Sending large number of this message to the CPU will influence the other tasks of the switch. To prevent the IP messages from attacking the CPU, a discarded entry is set to the hardware during the address resolution, so that all sequential messages with	

	that destination IP address are not sent to the CPU. After the address resolution, the entry is updated to the forwarding status, so that the switch could forward the message with that destination IP address in hardware. In general, during the ARP request ,if the switch CPU receives three destination IP address messages corresponding to the ARP entry, it is considered to be possible to attack the CPU and the switch sets the discarded entry to prevent the unknown unicast message from attacking the CPU. User could set the <i>num</i> parameter of this command to decide whether it attacks the CPU in specific network environment or disable this function. The arp anti-ip-attack function needs to occupy the switch hardware routing resources when attacked by the unknown unicast message. If there are enough resources, the arp anti-ip-attack num could be smaller. If not, in order to preferential ensure the use of the normal routing, the <i>num</i> could be larger or disable this function.					
Configuration Examples	The following example sets the IP message number that triggers to discard entry as 5. <pre>FS(config)# arp anti-ip-attack 5</pre> The following example disables the ARP anti-ip-attack function. <pre>FS(config)# arp anti-ip-attack 0</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

2.4 arp cache interface-limit

	Use this command to set the maximum number of ARP learned on the interface. Use the no form of this command to restore the default setting.	
	arp cache interface-limit <i>limit</i>	
	no arp cache interface-limit	
Parameter	Parameter	Description
Description	<i>limit</i>	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited.
Defaults	The default is 0.	
Command Mode	Interface configuration mode	
Usage Guide	This function can prevent ARP attacks from generating ARP entries to consume memory. <i>limit</i> must be no smaller than the number of ARPs learned on the interface. Otherwise, the configuration does not take effect.	
Configuration	The following example sets the maximum number of ARP learned on the interface to 300.	

Examples	<pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300</pre>	
	The following example restores the default setting. <pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# no arp cache interface-limit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.5 arp gratuitous-send interval

	Use this command to set the interval of sending the free ARP request message on the interface. Use the no form of this command to restore the default setting.	
	arp gratuitous-send interval <i>seconds</i>	
	no arp gratuitous-send	
Parameter Description	Parameter	Description
	<i>seconds</i>	The time interval to send the free ARP request message in the range from 1 to 3600 in the unit of seconds.
	<i>number</i>	The number of free ARP request message to be sent in the range from 1 to 100. The default value is 1.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the free ARP request message regularly on this interface to notify that the switch is the real gateway.	
Configuration Examples	The following example sets to send one free ARP request to SVI 1 per second. <pre>FS(config)# interface vlan 1 FS(config-if)# arp gratuitous-send interval 1</pre>	
	The following example stops sending the free ARP request to SVI 1. <pre>FS(config)# interface vlan 1 FS(config-if)# no arp gratuitous-send</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.6 arp oob

	Use this command to configure the static ARP on the management interface. Use the no form of this command to restore the default setting.	
	arp oob [<i>mgmt.-name</i>] <i>ip-address mac-address type</i>	
	no arp oob [<i>mgmt.-name</i>] <i>ip-address</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	The IP address corresponding to the MAC address, written as four groups of dotted decimal values.
	<i>mac-address</i>	The data link layer address, composed of 48 bits.
	<i>type</i>	The ARP encapsulation type. The key word for the Ethernet interface is arpa .
	<i>mgmt.-name</i>	Specifies the ARP-mapping management interface when there are multiple management interfaces.
Defaults	No static ARP is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS uses the ARP cache table to search for the 48-bit MAC address according to the 32-bit IP address. Most hosts support dynamic ARP analysis, so static ARP mapping does not need to be configured. The clear arp-cache oob command is used to clear the ARP mapping learned by the management port dynamically. If no management interface is specified, the static ARP is configured on the first management interface by default. If you specify the first management interface, the <i>mgmt.-name</i> parameter is not displayed by running the show run command.	
Configuration Examples	The following example configures a static ARP mapping record for the Ethernet host <pre>FS(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.7 arp proxy-resolved

	Use this command to enable a device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as an ARP proxy. Use the no form of this command to disable this function.	
	arp proxy-resolved	
	no arp proxy-resolved	

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After the arp proxy-resolved command is configured, the active VRRP device first judges, upon receiving an ARP request, whether the ARP entry corresponding to the destination IP address exists. If yes, the active VRRP device acts as an ARP proxy. If no, the active VRRP device does not act as an ARP proxy. In addition, the gateway automatically requests the ARP entry corresponding to the destination IP address in broadcast mode. This prevents a case that the gateway fails to act as a proxy to respond to an ARP request of the destination IP address due to absence of the ARP entry corresponding to the destination IP address. After the no arp proxy-resolved command is configured, if the proxy conditions are met, the active VRRP device directly acts as a proxy upon receiving an ARP request, with no need to judge whether the ARP entry corresponding to the destination IP address has been resolved.	
Configuration Examples	The following example disables a device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as an ARP proxy. <pre>FS(config)# no arp proxy-resolved</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.8 arp resolve vlan

	Use this command to enable active sending of ARP resolution requests to a specific sub VLAN of a super VLAN. Use the no form of this command to disable the active sending of ARP resolution requests to a specific sub VLAN of a super VLAN. Use the default form of this command to restore the default settings. arp resolve vlan {vlan-list none} no arp resolve vlan {vlan-list none} default arp resolve vlan	
Parameter Description	Parameter	Description
	vlan-list	Sets the list of sub VLANs in a super VLAN, where ARP resolution requests are sent only to these sub VLANs.
	none	Specifies that no ARP resolution request is sent to any sub VLAN of a super VLAN.

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	By default, the device actively sends ARP resolution requests to the entire super VLAN by default. If many sub VLANs exist in a super VLAN, then a great number of packet replications are caused and therefore affect device performance. Most terminals (such as PCs and servers) request ARP information from the gateway before accessing the network. Therefore, it is unnecessary to actively broadcast ARP resolution requests to the sub VLANs where these terminals reside. For dumb terminals that do not actively send free ARP requests, run the arp resolve vlan vlan-list command to actively send ARP resolution requests to VLANs in the specified VLAN list.  After the arp resolve vlan vlan-list command is configured, ARP resolution requests are sent only to VLANs specified in the VLAN list. It should be particularly noted that if authentication-free VLANs are not included in the VLAN list specified in the arp resolve vlan command, ARP resolution requests are not broadcast to the authentication-free VLANs.
Configuration Examples	The following example enables active sending of ARP resolution requests from the device to VLANs 10–20 and VLANs 25–30. <pre>FS(config)# arp resolve vlan 10-20, 25-30</pre> The following example disables active sending of ARP resolution requests from the device to VLANs 10–20. <pre>FS(config)# no arp resolve vlan 10-20</pre> The following example configures the device not to actively send ARP resolution requests to any sub VLAN of a super VLAN. <pre>FS(config)# arp resolve vlan none</pre>
Verification	Run the show running-config command to display configurations.

2.9 arp retry interval

	Use this command to set the frequency for sending the arp request message locally, namely, the time interval between two continuous ARP requests sent for resolving one IP address. Use the no form of this command to restore the default setting.	
	arp retry interval <i>seconds</i>	
	no arp retry interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Time for retransmitting the ARP request message in the range from 1 to 3600 in the unit of seconds.
Defaults	The default is 1.	
Command Mode	Global configuration mode.	

Usage Guide	The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry interval of the ARP request message longer. In general, it should not exceed the aging time of the dynamic ARP entry.	
Configuration Examples	The following example sets the retry interval of the ARP request as 30 seconds. FS(config)# arp retry interval 30	
Related Commands	Command	Description
	arp retry times	Number of times for retransmitting an ARP request message.
Platform Description	N/A	

2.10 arp retry times

	Use this command to set the local retry times of the ARP request message, namely, the times of sending the ARP request message to resolve one IP address. Use the no form of this command to restore the default setting.	
	arp retry times <i>number</i>	
	no arp retry times	
Parameter Description	Parameter	Description
	<i>number</i>	The times of sending the same ARP request in the range from 1 to 100. When it is set as 1, it indicates that the ARP request is not retransmitted, only 1 ARP request message is sent.
Defaults	The default is 5.	
Command Mode	Global configuration mode.	
Usage Guide	The switch sends the ARP request message frequently, and thus causing problems like network busy. In this case, you can set the retry times of the ARP request smaller. In general, the retry times should not be set too large.	
Configuration Examples	The following example sets the local ARP request not to be retried. FS(config)# arp retry times 1 The following example sets the local ARP request to be retried for one time. FS(config)# arp retry times 2	
Related Commands	Command	Description
	arp retry interval	Interval for retransmitting an ARP request message
Platform Description	N/A	

2.11 arp suppress-auth-vlan-req

	Use this command to disable the SVI interface from sending the ARP request to the authentication VLAN. Use the no form of this command to disable this function.	
	arp suppress-auth-vlan-req	
	no arp suppress-auth-vlan-req	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	In gateway authentication mode, all sub-VLANs of SuperVLAN are authentication VLANs by default. Users on authentication VLANs should pass the authentication before accessing the network. Static ARP table entries are generated on the device after users pass authentication. The device does not need to send ARP requests to the authentication VLAN when accessing these users. If the device accesses users on the authentication-exemption VLAN, it only needs to send ARP requests to the authentication-exemption VLAN. In gateway authentication mode, the device enables suppression of ARP request sent to the authentication VLAN by default. If the device needs to access authentication-exemption users on the authentication VLAN, this function should be disabled.	
Configuration Examples	The following example disables VLAN 2 from sending the ARP request to the authentication VLAN. <pre>FS(config)# interface vlan 2 FS(config-if-VLAN 2)# arp suppress-auth-vlan-req</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.12 arp switch-over resolve

	Use this command to enable active ARP resolution during active/standby switchovers in global configuration mode. Use the no form of this command to disable active ARP resolution during active/standby switchovers.	
	arp switch-over resolve	
	no arp switch-over resolve	
Parameter	Parameter	Description
Description	N/A	N/A

Defaults	Active ARP resolution during active/standby switchovers is disabled by default.
Command Mode	Global configuration mode
Default Level	2
Usage Guide	This command is used to quickly update ARP entries of the downlink device during stacking active/standby switchovers (especially when the downlink device is similar to a server with two NICs). When the standby host takes over the responsibilities of the active host, the new active host actively sends ARP resolution requests to a maximum of 1,000 terminals on a common SVI (not an interface in a super VLAN), to trigger the terminals to respond with ARP entries, thereby updating the ARP and MAC tables.
Configuration Examples	The following example enables active ARP resolution during active/standby switchovers. FS(config)# arp switch-over resolve
Verification	Run the show running-config command to display configurations.

2.13 arp timeout

	Use this command to configure the timeout for the ARP static mapping record in the ARP cache. Use the no form of this command to restore the default setting.	
	arp timeout <i>seconds</i>	
	no arp timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	The timeout is in the range from 0 to 2147483 in the unit of seconds.
Defaults	The default is 3600.	
Command Mode	Interface configuration mode/Global configuration mode	
Usage Guide	The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout unless there is a special requirement. The ARP timeout configuration in interface configuration mode prevail over that in global configuration mode.	
Configuration Examples	The following example sets the timeout for the dynamic ARP mapping record that is learned dynamically from FastEthernet port 0/1 to 120 seconds. FS(config)# interface fastEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# arp timeout 120 The following example sets the ARP timeout to 3000 seconds in global configuration mode.	

	FS(config)# arp timeout 3000	
Related Commands	Command	Description
	clear arp-cache	Clears the ARP cache list.
	show interface	Displays the interface information.
Platform Description	N/A	

2.14 arp trusted

	Use this command to set the maximum number of trusted ARP entries. Use the no form of this command to restore the default setting.	
	arp trusted <i>number</i>	
	no arp trusted	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of trusted ARP entries. It ranges from 10 to the maximum ARP volum minus 1,024.
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	To make this command valid, enable the trusted ARP function firstly. The trusted ARP entries and other entries share the memory. Too much trusted ARP entries may lead to insufficient ARP entry space. In general, you should set the maximum number of trusted ARP entries according to your real requirements.	
Configuration Examples	The following example sets 1000 trusted ARPs.	
	FS(config)# arp trusted 1000	
Related Commands	Command	Description
	service trustedarp	Enables the trusted ARP function.
Platform Description	N/A	

2.15 arp trust-monitor enable

	Use this command to enable egress gateway trusted ARP. Use the no form of this command to restore the default setting.	
	arp trust-monitor enable	
	no arp trust-monitor enable	

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	The egress gateway trusted ARP is different from GSN trusted ARP. With this function enabled, the device sends a unicast request for confirmation when learning an ARP table entry. The device learns the ARP table entry after receiving the response. When the device receives the ARP packet, only if the ARP table entry is aged or incomplete and the ARP packet is a response packet will the packet be handled. After egress gateway trusted ARP is enabled, the aging time of the ARP table entry turns to 60 seconds. After this function is disabled, the aging time restores to 3600 seconds.	
Configuration Examples	The following example enables egress gateway trusted ARP. <pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# arp trust-monitor enable</pre> The following example disables egress gateway trusted ARP. <pre>FS(config)# interface gi 0/0 FS(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.16 arp trusted aging

	Use this command to set trusted ARP aging. Use the no form of this command to restore the default setting.	
	arp trusted aging	
	no arp trusted aging	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	Use this command to set trusted ARP aging. Aging time is the same as dynamic ARP aging time. Use the arp timeout command to set aging time in interface mode.	

Configuration Examples	The following example enables trusted ARP aging. FS(config)# arp trusted aging	
Related Commands	Command	Description
	service trustedarp	Enables trusted ARP function.
Platform Description	N/A	

2.17 arp trusted user-vlan

	Use this command to execute the VLAN transformation while setting the trusted ARP entries. Use the no form of this command to restore the default setting.	
	arp trusted user-vlan <i>vid1</i> translated-vlan <i>vid2</i>	
	no arp trusted user-vlan <i>vid1</i>	
Parameter Description	Parameter	Description
	<i>vid1</i>	VID set by the server.
	<i>vid2</i>	VID after the transformation.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	In order to validate this command, enable the trusted ARP function first. This command is needed only when the VLAN sent by the server is different from the VLAN which takes effect in the trusted ARP entry.	
Configuration Examples	The following example sets the VLAN sent by the server to 3, but the VLAN which takes effect in the trusted ARP entry to 5. FS(config)# arp trusted user-vlan 3 translated-vlan 5	
Related Commands	Command	Description
	service trustedarp	Enables the trusted ARP function.
Platform Description	N/A	

2.18 arp unresolved

	Use this command to set the maximum number of the unresolved ARP entries. Use no form of this command to restore the default setting.	
	arp unresolved <i>number</i>	
	no arp unresolved	

Parameter	Parameter	Description
Description	<i>number</i>	The maximum number of the unresolved ARP entries in the range from 1 to the ARP table size supported by the device.
Defaults	The default is the ARP table size supported by the device.	
Command Mode	Global configuration mode.	
Usage Guide	If there are a large number of unresolved entries in the ARP cache table and they do not disappear after a period of time, this command can be used to limit the quantity of the unresolved entries.	
Configuration Examples	The following example sets the maximum number of the unresolved items to 500. FS(config)# arp unresolve 500	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.19 clear arp-cache

	Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table.	
	clear arp-cache [vrf <i>vrf_name</i> trusted] [ip [<i>mask</i>]] interface <i>interface-name</i>]	
Parameter	Parameter	Description
Description	trusted	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
	vrf <i>vrf_name</i>	Deletes dynamic ARP entries of the specified VRF instance. The default is the public instance.
	ip	Deletes ARP entries of the specified IP address. If <i>trusted</i> value is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
	mask	Deletes ARP entries in a subnet mask. If <i>trusted</i> value is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address is deleted by default.
	interface <i>interface-name</i>	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	This command can be used to refresh an ARP cache table. On a NFPP-based (Network Foundation Protection Policy) device, it receives one ARP packet for every mac/ip address per second by default. If the interval of two clear arp times is within 1s, the second response packet will be filtered and the ARP packet will not be resolved for a short time.					
Configuration Examples	The following example deletes all dynamic ARP mapping records. <pre>FS# clear arp-cache</pre> The following deletes the dynamic ARP entry 1.1.1.1. <pre>FS# clear arp-cache 1.1.1.1</pre> The following example deletes the dynamic ARP entry on interface SVI1. <pre>FS# clear arp-cache interface Vlan 1</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>arp</td><td>Adds a static mapping record to the ARP cache table.</td></tr></table>	Command	Description	arp	Adds a static mapping record to the ARP cache table.	
Command	Description					
arp	Adds a static mapping record to the ARP cache table.					
Platform Description	N/A					

2.20 clear arp-cache oob

	Use this command to clear dynamic ARP mapping records.	
	clear arp-cache oob [<i>ip</i> [<i>mask</i>]]	
Parameter	Parameter	Description
Description	<i>ip</i>	Clears the ARP table entry of the specified IP address. All dynamic ARP table entries are cleared by default.
	<i>mask</i>	Clears the ARP table entry within the specified subnet. The dynamic ARP table entry of the specified IP address (the previous parameter) is cleared by default.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	On a device supporting Network Foundation Protection Policy (NFPP), every MAC / IP address receives an ARP packet per second by default. If the clear arp oob command is run twice within one second, the second response packet may be filtered, causing ARP uanalysis for a short time.	
Configuration	The following example clears the cache table of dynamic ARP mapping records.	
Examples	FS# clear arp-cache oob	
	The following example clears dynamic ARP table entry 1.1.1.1.	

	FS# clear arp-cache oob 1.1.1.1 The following example clears the dynamic ARP table entry within the specified subnet. FS# clear arp-cache oob 1.0.0.0 255.0.0.0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.21 ip proxy-arp

	Use this command to enable ARP proxy function on the interface. Use the no form of this command to restore the default setting.	
	ip proxy-arp	
	no ip proxy-arp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.	
Configuration Examples	The following example enables ARP on FastEthernet port 0/1.	
	FS(config)# interface fastEthernet 0/1 FS(config-if)# ip proxy-arp	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.22 local-proxy-arp

	Use this command to enable local proxy ARP on the SVI interface. Use the no form of this command to restore the default setting.

	local-proxy-arp	
	no local-proxy-arp	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	With local proxy ARP enabled, the device helps a host to obtain MAC addresses of other hosts on the subnet. If the device enables switchport protected, users on different ports are segregated on layer 2. After local proxy ARP is enabled, the device serves as a proxy to send a response after receiving an ARP request. The ARP response contains a MAC address which is the device's Ethernet MAC address, realizing communication between different hosts through L3 routes.	
Configuration Examples	The following example enables local proxy ARP on VLAN1. <pre>FS(config)# interface vlan 1 FS(config-if-VLAN 1)# local-proxy-arp</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.23 service trustedarp

	Use this command to enable the trusted ARP function. Use the no form of this command to restore the default setting.	
	service trustedarp	
	no service trustedarp	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The trusted ARP function of the device is to prevent the ARP fraud function. As a part of the GSN scheme, it should be used together with the GSN scheme.	

Configuration Examples	The following example enables the trusted ARP function in global configuration mode. FS(config)# service trustedarp	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.24 show arp

	Use this command to display the Address Resolution Protocol (ARP) cache table	
	show arp [<i>interface-type interface-number</i> trusted [<i>ip</i> [<i>mask</i>]] [vrf <i>vrf-name</i>] [<i>ip</i> [<i>mask</i>] <i>mac-address</i> static complete incomplete]]	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Displays the ARP entry of a specified Layer-2 or Layer-3 port.
	<i>interface-number</i>	
	vrf <i>vrf_name</i>	VRF instance, which Displays the ARP entry with specified VRF.
	trusted	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.
	<i>ip</i>	Displays the ARP entry of the specified IP address. If trusted is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	<i>mask</i>	Displays the ARP entries of the network segment included within the mask. If trusted is configured, only trusted ARP entries are displayed. Otherwise, untrusted ARP entries are displayed.
	static	Displays all the static ARP entries.
	complete	Displays all the resolved dynamic ARP entries.
	incomplete	Displays all the unresolved dynamic ARP entries.
	<i>mac-address</i>	Displays the ARP entry with the specified mac address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the output result of the show arp command: FS# show arp Total Numbers of Arp: 7 Protocol Address Age(min) Hardware Type Interface Internet 192.168.195.68 0 0013.20a5.7a5f arpa VLAN 1 Internet 192.168.195.67 0 001a.a0b5.378d arpa VLAN 1	

```
Internet 192.168.195.65 0 0018.8b7b.713e arpa VLAN 1
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.63 0 001a.a0b5.3990 arpa VLAN 1
Internet 192.168.195.62 0 001a.a0b5.0b25 arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
```

The following example displays the output result of `show arp 192.168.195.68`

```
FS# show arp 192.168.195.68
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.68 1 0013.20a5.7a5f arpa VLAN 1
```

The following example displays the output result of `show arp 192.168.195.0 255.255.255.0`

```
FS# show arp 192.168.195.0 255.255.255.0
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.64 0 0018.8b7b.9106 arpa VLAN 1
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa VLAN 1
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa VLAN 1
Internet 192.168.195.51 1 0018.8b82.8691 arpa VLAN 1
```

The following example displays the output result of `show arp 001a.a0b5.378d`

```
FS# show arp 001a.a0b5.378d
Protocol Address Age(min) Hardware Type Interface
Internet 192.168.195.67 4 001a.a0b5.378d arpa VLAN 1
```

The following example displays the output result of `show arp static`.

```
FS# show arp static
Protocol Address Age(min) Hardware Type Interface Origin
Internet 192.168.23.55 <static> 0000.0000.0010 arpa VLAN 100 Configure
Internet 192.168.23.56 <static> 0000.0000.0020 arpa VLAN 100 Authentication
Internet 192.168.23.57 <static> 0000.0000.0020 arpa VLAN 100 DHCP-Snooping
2 static arp entries exist.
```

The meaning of each field in the ARP cache table is described as below:

Table 1 Fields in the ARP cache table

Field	Description
Protocol	Protocol of the network address, always to be Internet
Address	IP address corresponding to the hardware address
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "--".
Hardware	Hardware address corresponding to the IP address
Type	Hardware address type, ARPA for all Ethernet addresses

	Interface	Interface associated with the IP addresses
	Origin	Origin of static ARP entries.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.25 show arp counter

	Use this command to display the number of ARP entries in the ARP cache table.	
	show arp counter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the output result of the show arp counter command: <pre>FS#sho arp counter ARP Limit: 75000 Count of static entries: 0 Count of dynamic entries: 1 (complete: 1 incomplete: 0) Total: 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.26 show arp detail

	Use this command to display the details of the Address Resolution Protocol (ARP) cache table.
	show arp detail [<i>interface-type interface-number</i> trusted [<i>ip [mask]</i>] [vrf <i>vrf-name</i>] [<i>ip [mask]</i> <i>mac-address</i>] static complete incomplete] subvlan { <i>subvlan-number</i> min-max <i>min_value max_value</i> }

Parameter Description	Parameter	Description																																																																											
	<i>interface-type interface-number</i>	Displays the ARP of the layer 2 port or the layer 3 interface.																																																																											
	<i>vrf vrf_name</i>	VRF instance, which Displays the ARP entry with specified VRF.																																																																											
	<i>trusted</i>	Displays the trusted ARP entries. Currently, only the global VRF supports the trusted ARP.																																																																											
	<i>ip</i>	Displays the ARP entry of the specified IP address.																																																																											
	<i>ip mask</i>	Displays the ARP entries of the network segment included within the mask.																																																																											
	<i>mac-address</i>	Displays the ARP entry of the specified MAC address.																																																																											
	<i>static</i>	Displays all the static ARP entries.																																																																											
	<i>complete</i>	Displays all the resolved dynamic ARP entries.																																																																											
	<i>incomplete</i>	Displays all the unresolved dynamic ARP entries.																																																																											
	<i>subvlan</i>	Displays the ARP entries of the specified subvlan																																																																											
	<i>subvlan-number</i>	Subvlan ID																																																																											
	<i>min-max</i>	Displays the minimum and maxinum subvlan ID																																																																											
	<i>min_value</i>	Minimum subvlan ID																																																																											
	<i>max_value]</i>	Maximum subvlan ID.																																																																											
Defaults	N/A																																																																												
Command Mode	Privileged EXEC mode																																																																												
Usage Guide	Use this command to display the ARP details, such as the ARP type (Dynamic, Static, Local, Trust), the information on the layer2 port. If you enter a <i>min_value</i> greater than <i>max_value</i> , no error message is prompted. Instead, ARP entries corresponding to the subvlan are displayed.																																																																												
Configuration Examples	The following example displays the output result of the show arp detail command: FS# show arp detail<table><tr><th>IP Address</th><th>MAC Address</th><th>Type</th><th>Age(min)</th><th>Interface</th><th>Port</th><th>SubVlan</th></tr><tr><td>20.1.1.2</td><td>0020.0101.0002</td><td>Static</td><td>--</td><td>Te2/5</td><td>--</td><td>--</td></tr><tr><td>20.1.1.1</td><td>00d0.f822.33bb</td><td>Local</td><td>--</td><td>Te2/5</td><td>--</td><td>--</td></tr><tr><td>1.1.1.2</td><td>00d0.1111.1112</td><td>Dynamic</td><td>1</td><td>VI2</td><td>Te2/1</td><td>4</td></tr><tr><td>1.1.1.1</td><td>00d0.f822.33bb</td><td>Local</td><td>--</td><td>VI2</td><td>--</td><td>--</td></tr></table> The following example displays arp details including InnerVLAN on products supporting QinQ termination: FS# show arp detail<table><tr><th>IP Address</th><th>MAC Address</th><th>Type</th><th>Age(min)</th><th>Interface</th><th>Port</th><th>SubVlan</th><th>InnerVlan</th></tr><tr><td>20.1.1.2</td><td>0020.0101.0002</td><td>Static</td><td>--</td><td>Te2/5</td><td>--</td><td>--</td><td></td></tr><tr><td>20.1.1.1</td><td>00d0.f822.33bb</td><td>Local</td><td>--</td><td>Te2/5</td><td>--</td><td>--</td><td></td></tr><tr><td>1.1.1.2</td><td>00d0.1111.1112</td><td>Dynamic</td><td>1</td><td>VI2</td><td>Te2/1</td><td>4</td><td>300</td></tr><tr><td>1.1.1.1</td><td>00d0.f822.33bb</td><td>Local</td><td>--</td><td>VI2</td><td>--</td><td>--</td><td></td></tr></table>		IP Address	MAC Address	Type	Age(min)	Interface	Port	SubVlan	20.1.1.2	0020.0101.0002	Static	--	Te2/5	--	--	20.1.1.1	00d0.f822.33bb	Local	--	Te2/5	--	--	1.1.1.2	00d0.1111.1112	Dynamic	1	VI2	Te2/1	4	1.1.1.1	00d0.f822.33bb	Local	--	VI2	--	--	IP Address	MAC Address	Type	Age(min)	Interface	Port	SubVlan	InnerVlan	20.1.1.2	0020.0101.0002	Static	--	Te2/5	--	--		20.1.1.1	00d0.f822.33bb	Local	--	Te2/5	--	--		1.1.1.2	00d0.1111.1112	Dynamic	1	VI2	Te2/1	4	300	1.1.1.1	00d0.f822.33bb	Local	--	VI2	--	--	
IP Address	MAC Address	Type	Age(min)	Interface	Port	SubVlan																																																																							
20.1.1.2	0020.0101.0002	Static	--	Te2/5	--	--																																																																							
20.1.1.1	00d0.f822.33bb	Local	--	Te2/5	--	--																																																																							
1.1.1.2	00d0.1111.1112	Dynamic	1	VI2	Te2/1	4																																																																							
1.1.1.1	00d0.f822.33bb	Local	--	VI2	--	--																																																																							
IP Address	MAC Address	Type	Age(min)	Interface	Port	SubVlan	InnerVlan																																																																						
20.1.1.2	0020.0101.0002	Static	--	Te2/5	--	--																																																																							
20.1.1.1	00d0.f822.33bb	Local	--	Te2/5	--	--																																																																							
1.1.1.2	00d0.1111.1112	Dynamic	1	VI2	Te2/1	4	300																																																																						
1.1.1.1	00d0.f822.33bb	Local	--	VI2	--	--																																																																							

	The meaning of each field in the ARP cache table is described as below:																							
	Table 1 Fields in the ARP cache table																							
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>IP Address</td><td>IP address corresponding to the hardware address</td></tr><tr><td>MAC Address</td><td>hardware address corresponding to the IP address</td></tr><tr><td>Age (min)</td><td>Age of the ARP learning, in minutes</td></tr><tr><td>Port</td><td>Layer2 port associated with the ARP</td></tr><tr><td>Type</td><td>ARP type, includes the Static, Dynamic, Trust,Local</td></tr><tr><td>Interface</td><td>Layer 3 interface associated with the IP addresses</td></tr><tr><td>SubVLAN</td><td>SubVLAN corresponding to the ARP entries</td></tr><tr><td>InnerVLAN</td><td>InnerVLAN or CE-VLAN corresponding to the ARP entries</td></tr><tr><td>Subvni</td><td>Vni corresponding to the ARP entries, namely ID of the VxLAN.</td></tr><tr><td>Location</td><td>Local: ARP entries are generated or learned on the local device. Remote: ARP entries are synced from a remote gateway.</td></tr></table>	Field	Description	IP Address	IP address corresponding to the hardware address	MAC Address	hardware address corresponding to the IP address	Age (min)	Age of the ARP learning, in minutes	Port	Layer2 port associated with the ARP	Type	ARP type, includes the Static, Dynamic, Trust,Local	Interface	Layer 3 interface associated with the IP addresses	SubVLAN	SubVLAN corresponding to the ARP entries	InnerVLAN	InnerVLAN or CE-VLAN corresponding to the ARP entries	Subvni	Vni corresponding to the ARP entries, namely ID of the VxLAN.	Location	Local: ARP entries are generated or learned on the local device. Remote: ARP entries are synced from a remote gateway.	
Field	Description																							
IP Address	IP address corresponding to the hardware address																							
MAC Address	hardware address corresponding to the IP address																							
Age (min)	Age of the ARP learning, in minutes																							
Port	Layer2 port associated with the ARP																							
Type	ARP type, includes the Static, Dynamic, Trust,Local																							
Interface	Layer 3 interface associated with the IP addresses																							
SubVLAN	SubVLAN corresponding to the ARP entries																							
InnerVLAN	InnerVLAN or CE-VLAN corresponding to the ARP entries																							
Subvni	Vni corresponding to the ARP entries, namely ID of the VxLAN.																							
Location	Local: ARP entries are generated or learned on the local device. Remote: ARP entries are synced from a remote gateway.																							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A																			
Command	Description																							
N/A	N/A																							
Platform Description	N/A																							

2.27 show arp oob

Use this command to display the ARP cache table.		
show arp oob [<i>ip</i> [<i>mask</i>] static complete incomplete <i>mac-address</i>]		
Parameter Description	Parameter	Description
	<i>ip</i>	Displays ARP table entries of the specified IP address.
	<i>mask</i>	Displays ARP table entries within the IP subnet.
	static	Displays all static ARP table entries.
	complete	Displays all analyzed ARP table entries.
	incomplete	Displays all unanalyzed ARP table entries.
	<i>mac-address</i>	Displays ARP table entries of the specified MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the ARP cache table. The complete / incomplete key word represents analyzed / unanalyzed ARP table entries.	

Configuration Examples	The following example displays the outcome of the running the show arp oob command.					
	FS# show arp oob					
	Total Numbers of Arp: 7					
	Protocol	Address	Age(min)	Hardware	Type	Interface
	Internet	192.168.195.68	0	0013.20a5.7a5f	arpa	mgmt 0
	Internet	192.168.195.67	0	001a.a0b5.378d	arpa	mgmt 0
	Internet	192.168.195.65	0	0018.8b7b.713e	arpa	mgmt 0
	Internet	192.168.195.64	0	0018.8b7b.9106	arpa	mgmt 0
	Internet	192.168.195.63	0	001a.a0b5.3990	arpa	mgmt 0
	Internet	192.168.195.62	0	001a.a0b5.0b25	arpa	mgmt 0
	Internet	192.168.195.5	--	00d0.f822.33b1	arpa	mgmt 0
The following example displays the outcome of running the show arp oob 192.168.195.68 command.						
FS# show arp oob 192.168.195.68						
Protocol Address Age(min) Hardware Type Interface						
Internet 192.168.195.68 1 0013.20a5.7a5f arpa mgmt 0						
The following example displays the outcome of running the show arp oob 192.168.195.0 255.255.255.0 command.						
FS# show arp 192.168.195.0 255.255.255.0						
Protocol Address Age(min) Hardware Type Interface						
Internet 192.168.195.64 0 0018.8b7b.9106 arpa mgmt 0						
Internet 192.168.195.2 1 00d0.f8ff.f00e arpa mgmt 0						
Internet 192.168.195.5 -- 00d0.f822.33b1 arpa mgmt 0						
Internet 192.168.195.1 0 00d0.f8a6.5af7 arpa mgmt 0						
Internet 192.168.195.51 1 0018.8b82.8691 arpa mgmt 0						
The following example displays the outcome of running the show arp oob 001a.a0b5.378d command.						
FS# show arp 001a.a0b5.378d						
Protocol Address Age(min) Hardware Type Interface						
Internet 192.168.195.67 4 001a.a0b5.378d arpa mgmt 0						
Field			Description			
Protocol			Only "Internet" is available at present, which indicates the IP protocol.			
Address			The IPv4 address.			
Age(min)			The age of the table entry. For the local IP address, the field is displayed as '-'. For the static table entry, the field is displayed as <static>. For the dynamic table entry, the field indicates the time for which the table entry has been learned, in the unit of minutes.			
Hardware			48-bit MAC address, written as a dotted triple of four-digit hexadecimal numbers.			
Type			Only "arpa" is available at present.			

	Interface	The L3 interface corresponding to the ARP table entry. The field is NULL for static ARP table entries for the IP address of the static ARP is not within any network segment directly connected with the device.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.28 show arp packet statistics

	Use this command to display the statistics of ARP packets.					
	show arp packet statistics [<i>interface-name</i>]					
Parameter	Parameter			Description		
Description	<i>interface-name</i>			Displays the statistics of ARP packets on the specified interface.		
Defaults	N/A.					
Command Mode	Privileged EXEC mode.					
Usage Guide	N/A.					
Configuration Examples	The following example displays the output information of the command.					
	FS#show arp packet statistics					
	Interface		Received	Received	Received	Sent
	Name		R			Sent
	equests	Replies	Others	Requests	Replies	
	-----	-----	-----	-----	-----	
	GigabitEthernet 0/0		0	0	0	0
	GigabitEthernet 0/1		143649	232	0	2
	GigabitEthernet 0/2		0	0	0	0
	GigabitEthernet 0/3		0	0	0	0
	GigabitEthernet 0/4		0	0	0	0
	GigabitEthernet 0/5		0	0	0	0
	GigabitEthernet 0/6		0	0	0	0
	Loopback 1		0	0	0	0
	Description of fields:					
	Field			Description		
	Received Requests			Number of received ARP requests		
	Received Replies			Number of received ARP response messages		

	Received Others	Number of other received ARP packets	
	Sent Requests	Number of sent ARP requests	
	Sent Replies	Number of sent ARP requests	
Related Commands	Command	Description	
	N/A.	N/A.	
Platform Description	N/A		

2.29 show arp timeout

	Use this command to display the aging time of a dynamic ARP entry on the interface.	
	show arp timeout	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	N/A.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A.	
Configuration Examples	The following example displays the output of the show arp timeout command: <pre>FS# show arp timeout Interface arp timeout(sec) ----- VLAN 1 3600</pre> The meaning of each field in the ARP cache table is described in Table 1.	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A	

2.30 show ip arp

	Use this command to display the Address Resolution Protocol (ARP) cache table.
	show ip arp [vrf vrf-name]

Parameter	Parameter	Description														
Description	vrf-name	VRF instance.														
Defaults	N/A.															
Command Mode	Privileged EXEC mode.															
Usage Guide	N/A.															
Configuration Examples	The following example displays the output of show ip arp: <pre>FS# show ip arp Protocol Address Age(min) Hardware Type Interface Internet 192.168.7.233 23 0007.e9d9.0488 ARPA FastEthernet 0/0 Internet 192.168.7.112 10 0050.eb08.6617 ARPA FastEthernet 0/0 Internet 192.168.7.79 12 00d0.f808.3d5c ARPA FastEthernet 0/0 Internet 192.168.7.1 50 00d0.f84e.1c7f ARPA FastEthernet 0/0 Internet 192.168.7.215 36 00d0.f80d.1090 ARPA FastEthernet 0/0 Internet 192.168.7.127 0 0060.97bd.ebee ARPA FastEthernet 0/0 Internet 192.168.7.195 57 0060.97bd.ef2d ARPA FastEthernet 0/0 Internet 192.168.7.183 -- 00d0.f8fb.108b ARPA FastEthernet 0/0</pre> The following example displays the output of show ip arp vrf vpnv4. <pre>FS#show ip arp vrf vpnv4 Protocol Address Age(min) Hardware Type Interface Internet 11.1.1.1 0 78e3.b5b6.f4dc arpa GigabitEthernet 0/0 Internet 11.1.1.2 -- 1111.2222.1111 arpa GigabitEthernet 0/0 Total number of ARP entries: 2</pre> Each field in the ARP cache table has the following meanings: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Protocol</td><td>Network address protocol, always Internet.</td></tr><tr><td>Address</td><td>The IP address corresponding to the hardware address.</td></tr><tr><td>Age (min)</td><td>Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".</td></tr><tr><td>Hardware</td><td>Hardware address corresponding to the IP address</td></tr><tr><td>Type</td><td>The type of hardware address. The value is ARPA for all Ethernet addresses.</td></tr><tr><td>Interface</td><td>Interface associated with the IP address.</td></tr></table>		Field	Description	Protocol	Network address protocol, always Internet.	Address	The IP address corresponding to the hardware address.	Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".	Hardware	Hardware address corresponding to the IP address	Type	The type of hardware address. The value is ARPA for all Ethernet addresses.	Interface	Interface associated with the IP address.
Field	Description															
Protocol	Network address protocol, always Internet.															
Address	The IP address corresponding to the hardware address.															
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".															
Hardware	Hardware address corresponding to the IP address															
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.															
Interface	Interface associated with the IP address.															
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A.</td><td>N/A.</td></tr></table>	Command	Description	N/A.	N/A.											
Command	Description															
N/A.	N/A.															
Platform Description	N/A															

3 IPv6 Commands

3.1 clear ipv6 neighbors

	Use this command to clear the dynamic IPv6 neighbors.	
	clear ipv6 neighbors [vrf <i>vrf-name</i>] [oob] [<i>interface-id</i>]	
Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name. All global IPv6 neighbors are cleared without specified VRF name by default.
	oob	Clears the dynamic IPv6 neighbors discovered by neighbors on MGMT interface.
	<i>interface-id</i>	Interface name. Clear the dynamically learned IPv6 neighbors on the specified interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command does not clear all the dynamic neighbors on authentication VLAN. Note that the static neighbors will not be cleared.	
Configuration Examples	The following example clears the dynamic IPv6 neighbors. <pre>FS# clear ipv6 neighbors</pre> The following example clears all dynamic neighbors on the MGMT port. <pre>FS# clear ipv6 neighbors oob</pre> The following example clears all dynamic neighbors on the interface gigabitEthernet 0/1. <pre>FS# clear ipv6 neighbors gigabitEthernet 0/1</pre>	
Related Commands	Command	Description
	ipv6 neighbor	Configures the neighbor.
	show ipv6 neighbors	Displays the neighbor information.
Platform Description	N/A	

3.2 ipv6 address

	Use this command to configure an IPv6 address for a network interface. Use the no form of this command to

	restore the default setting.	
	ipv6 address <i>ipv6-address/prefix-length</i>	
	ipv6 address <i>ipv6-prefix/prefix-length eui-64</i>	
	ipv6 address <i>prefix-name sub-bits/prefix-length [eui-64]</i>	
	no ipv6 address	
	no ipv6 address <i>ipv6-address/prefix-length</i>	
	no ipv6 address <i>ipv6-prefix/prefix-length eui-64</i>	
	no ipv6 address <i>prefix-name sub-bits/prefix-length [eui-64]</i>	
Parameter	Parameter	Description
Description	<i>iipv6-prefix</i>	IPv6 address prefix in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>ipv6-address</i>	IPv6 address in the format defined in RFC4291. The address shall be in hex; the fields in the address shall be separated by comma, and each field shall contain 16 bits.
	<i>prefix-length</i>	Length of the IPv6 prefix, the network address of the IPv6 address. Note: The prefix length range of the IPv6 address of the interface of S86 is 0 to 64 or 128 to 128.
	<i>prefix-name</i>	The general prefix name. Use the specified general prefix to generate the interface address.
	<i>sub-bits</i>	The value of the sub-prefix bit and the host bit generates the interface address combining with the general prefix. The value shall be in the format defined in the RFC4291.
	eui-64	The generated IPV6 address consists of the address prefix and the 64 bit interface ID
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	When an IPv6 interface is created and the link status is UP, the system will automatically generate a local IP address for the interface. The IPv6 address could also be generated using the general prefix. That is, the IPv6 address consists of the general prefix and the sub-prefix and the host bit. The general prefix could be configured using the ipv6 general-prefix command or may be learned through the DHCPv6 agent PD (Prefix Discovery) function (please refer to the <i>DHCPv6 Configuration</i>). Use the <i>sub-bits/prefix-length</i> parameter of this command to configure the sub-prefix and the host bit. If no deleted address is specified when using no ipv6 address, all the manually configured addresses will be deleted. The no ipv6 address ipv6-prefix/prefix-length eui-64 command can be used to delete the addresses configured with ipv6 address ipv6-prefix/prefix-length eui-64.	

Configuration Examples	The following example configures an IPv6 address for the interface GigabitEthernet 0/1. <pre>FS(config-if)# ipv6 address 2001:1::1/64 FS(config-if)# no ipv6 address 2001:1::1/64 FS(config-if)# ipv6 address 2002:1::1/64 eui-64 FS(config-if)# no ipv6 address 2002:1::1/64 eui-64</pre> The following example applies general prefix to configure an IPv6 address for the interface GigabitEthernet 0/1. <pre>FS(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix 0:0:0:7272::72/64</pre>  If the prefix 2001:1111:2222::/48 is configured under the general prefix name <i>my-prefix</i>, then the generated IPv6 address of the interface is 2001:1111:2222:7272::72/64.					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

3.3 ipv6 address autoconfig

	Use this command to automatically configure an IPv6 stateless address for a network interface. Use the no form of this command to restore the default setting.	
	ipv6 address autoconfig [default]	
	no ipv6 address autoconfig	
Parameter	Parameter	Description
Description	default	(Optional) If this keyword is configured, a default routing is generated. Note that only one layer3 interface on the entire device is allowed to use the default keyword
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	The stateless automatic address configuration is that when receiving the RA (Route Advertisement) message, the device could use the prefix information of the RA message to automatically generate the EUI-64 interface address. If the RA message contains the flag of the “other configurations”, the interface will obtain these “other configurations” through the DHCPv6. The “other configurations” usually means the IPv6 address of the DNS server, the IPv6 address of the NTP server, etc. Use the no ipv6 address autoconfig command to delete the IPv6 address.	
Configuration Examples	The following example automatically configures an IPv6 stateless address for a network interface and generates a default route.	

	FS(config-if-GigabitEthernet 0/1)# ipv6 address autoconfig default	
	The following example restores the default setting.	
	FS(config-if-GigabitEthernet 0/1)# no ipv6 address autoconfig	
Related Commands	Command	Description
	ipv6 address ipv6-prefix/prefix-length [eui-64]	Configures the IPv6 address for the interface manually.
Platform Description	N/A	

3.4 ipv6 icmp error-interval

	Use this command to set the frequency with which ICMPv6-oversize error packets are sent. Use the no form of this command to restore the default setting.	
	ipv6 icmp error-interval too-big <i>milliseconds</i> [<i>bucket-size</i>]	
	no ipv6 icmp error-interval too-big <i>milliseconds</i> [<i>bucket-size</i>]	
	Use this command to set the frequency with which other ICMPv6 error packets are sent. Use the no form of this command to restore the default setting.	
	ipv6 icmp error-interval <i>milliseconds</i> [<i>bucket-size</i>]	
	no ipv6 icmp error-interval <i>milliseconds</i> [<i>bucket-size</i>]	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	Sets the refresh interval of the token bucket, in the range from 0 to 2147483647 in the unit of seconds. Setting the value to 0 indicates that the frequency with which ICMPv6 error packets are sent is not fixed.
	<i>bucket-size</i>	Sets the number of tokens in the token bucket, in the range from 1 to 200.
Defaults	The default <i>milliseconds</i> is 100 and <i>bucket-size</i> is 10.	
Command Mode	Global configuration mode	
Usage Guide	The token bucket algorithm is adopted to set the frequency with which ICMPv6 error packets are sent so as to prevent Denial of Service (DoS) attack, If the forwarded IPv6 packet is greater than the egress IPv6 MTU in size, the router discards the IPv6 packet and sends the ICMPv6-oversize error packet to the source IPv6 address. This kind of ICMPv6 error packet is used for IPv6 path MTU discovery. If there are too many ICMPv6 error packets, the ICMPv6-oversize error packet may not be sent, causing IPv6 path MTU discovery failure. Therefore, it is recommended to set the frequency of ICMPv6-oversize error packet and other ICMPv6 error packet respectively. Note that ICMPv6 redirect packet is not an ICMPv6 error packet and FS sets the frequency of the ICMPv6 redirect packet the same as that of other ICMPv6	

	error packet. For the timer is accurate to 10 milliseconds, it is recommended to set the refresh interval of the token bucket to an integer multiple of 10 milliseconds. If the refresh interval is not an integer multiple of 10 milliseconds, it is converted automatically. For example, the frequency of 1 per five milliseconds turns out to be 2 per 10 milliseconds; the frequency of 3 per 15 milliseconds is converted to 2 per 10 milliseconds.							
Configuration Examples	The following example sets the frequency with which ICMPv6-oversize error packets are sent to 100 per second. <pre>FS(config)# ipv6 icmp error-interval too-big 1000 100</pre> The following example sets the frequency with which other ICMPv6 error packets are sent to 10 per second. <pre>FS(config)# ipv6 icmp error-interval 1000 10</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr><tr><td></td><td></td></tr></table>	Command	Description	N/A	N/A			
Command	Description							
N/A	N/A							
Platform Description	N/A							

3.5 ipv6 enable

	Use this command to enable the IPv6 function on an interface. Use the no form of this command to restore the default setting.	
	ipv6 enable	
	no ipv6 enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	The IPv6 function of an interface can be enabled by configuring ipv6 enable or by configuring IPv6 address for the interface.  If an IPv6 address is configured for the interface, the IPv6 function will be enabled automatically on the interface and cannot be disabled with no ipv6 enable.	
Configuration Examples	The following example enables the IPv6 function on the interface GigabitEthernet 0/1. <pre>FS(config-if-GigabitEthernet 0/1)# ipv6 enable</pre>	
Related Commands	Command	Description
	show ipv6 interface	Displays the related information of an interface.

Platform	N/A
Description	

3.6 ipv6 gateway

	Use this command to configure the default gateway IPv6 address on the management port.	
	ipv6 gateway <i>ipv6-address</i>	
Parameter	Parameter	Description
Description	ipv6-address	Configures the default gateway IPv6 address.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	The management port is MGMT in type and 0 in ID.	
Configuration Examples	The following example configures the default gateway IPv6 address on the management port. <pre>FS(config)# interface mgmt 0 FS(config-int)# ipv6 gateway 2001::1 FS(config-int)# exit FS(config)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

3.7 ipv6 general-prefix

	Use this command to configure the IPv6 general prefix in the global configuration mode.	
	ipv6 general-prefix <i>prefix-name ipv6-prefix/prefix-length</i>	
	no ipv6 general-prefix <i>prefix-name ipv6-prefix/prefix-length</i>	
Parameter	Parameter	Description
Description	prefix-name	The general prefix name.
	ipv6-prefix	The network prefix value of the general-prefix following the format defined in RFC4291.
	prefix-length	The length of the general prefix.
Defaults	N/A	

Command Mode	Global configuration mode.	
Usage Guide	It is convenient to number the network by using the general prefix, which defines a prefix so that many longer specified prefixes could refer to it. These specified prefixes are updated whenever the general prefix changes. If the network number changes, just modify the general prefix. A general prefix could contain multiple prefixes. These longer specified prefixes are usually used for the ipv6 address configuration on the interface.	
Configuration Examples	The following example configures manually a general prefix as my-prefix. <pre>FS(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48</pre>	
Related Commands	Command	Description
	ipv6 address prefix-name sub-bits/prefix-length	Configures the interface address using the general prefix.
	show ipv6 general-prefix	Displays the general prefix.
Platform Description	N/A	

3.8 ipv6 hop-limit

	Use this command to configure the default hopcount to send unicast messages in the global configuration mode.	
	ipv6 hop-limit <i>value</i>	
	no ipv6 hop-limit	
Parameter Description	Parameter	Description
	<i>value</i>	Hopcount ranging from 1 to 255.
Defaults	The default is 64.	
Command Mode	Global configuration mode.	
Usage Guide	This command takes effect for the unicast messages only, not for multicast messages.	
Configuration Examples	The following example sets the default hopcount to 100. <pre>FS(config)# ipv6 hop-limit 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.9 ipv6 mtu

	Use this command to configure the MTU of IPv6 packets. Use the no form of this command to restore the default setting.	
	ipv6 mtu <i>bytes</i>	
	no ipv6 mtu	
Parameter Description	Parameter	Description
	<i>bytes</i>	MTU of IPv6 packets, in bytes. The value ranges from 1,280 to 1,500.
Defaults	The default configuration is the same as the configuration of the mtu command.	
Command Mode	Interface configuration mode	
Usage Guide	If the size of an IPv6 packet exceeds the IPv6 MTU, the FSOS software segments the packet. For all devices in the same physical network segment, the IPv6 MTU of the interconnected interface must be the same.	
Configuration Examples	The following example sets the IPv6 MTU of the FastEthernet 0/1 interface to 1400 bytes.	
	<pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# ipv6 mtu 1400</pre>	
Related Commands	Command	Description
	mtu	Sets the MTU of an interface.
Platform Description	This command cannot be used on Layer 2 devices.	

3.10 ipv6 nd cache interface-limit

	Use this command to set the maximum number of neighbors learned on the interface. Use the no form of this command to restore the default setting.	
	ipv6 nd cache interface-limit <i>value</i>	
	no ipv6 nd cache interface-limit	
Parameter Description	Parameter	Description
	<i>value</i>	Sets the maximum number of neighbors learned on the interface, including the static and dynamic neighbors, in the range from 0 to the number supported by the device. 0 indicates the number is not limited.
Defaults	The default is 0.	
Command	Interface configuration mode	

Mode						
Usage Guide	This function can prevent neighbor entries generated by malicious neighbor attacks from consuming memory. <i>limit</i> must be no smaller than the number of neighbors learned on the interface. Otherwise, the configuration does not take effect.					
Configuration Examples	The following example sets the number of neighbors learned on the interface to 100. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

3.11 ipv6 nd dad attempts

	Use this command to set the number of the NS packets to be continuously sent for IPv6 address collision check on the interface. Use the no form of this command to restore it to the default setting.					
	ipv6 nd dad attempts <i>value</i>					
	no ipv6 nd dad attempts <i>value</i>					
Parameter Description	<table><tr><th>Parameter</th><th>Description</th></tr><tr><td><i>value</i></td><td>Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.</td></tr></table>	Parameter	Description	<i>value</i>	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.	
Parameter	Description					
<i>value</i>	Number of the NS packets. If it is set to 0, it indicates that the IPv6 address collision check is disabled on the interface. The range is 0 to 600.					
Defaults	The default is 1.					
Command Mode	Interface configuration mode.					
Usage Guide	When the interface is configured with a new IPv6 address, the address collision shall be checked before the address is assigned to the interface, and the address shall be in the "tentative" status. After the address collision check is completed, if no collision is detected, the address can be used normally; if collision is detected and the interface ID of the address is an EUI-64 ID, it indicates that the link-layer address is repeated, and the system will automatically shut down the interface (that is, to prohibit IPv6 operations on the interface). In this case, you shall modify and configure a new address manually, and restart address collision check for the down/up interface. Whenever the state of an interface changes from down to up, the address collision check function of the interface will be enabled.					
Configuration Examples	The following example sets the number of the NS packets.					
	FS(config-if-GigabitEthernet 0/1)# ipv6 nd dad attempts 3					

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
Platform Description	N/A	

3.12 ipv6 nd dad retry

	Use this command to set the interval for address conflict detection. Use the no form of this command to restore the default setting.	
	ipv6 nd dad retry <i>value</i>	
	no ipv6 nd dad retry	
Parameter Description	Parameter	Description
	<i>value</i>	Sets the interval for address conflict detection, 60 seconds by default. Setting <i>value</i> to 0 indicates that the function is disabled.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Before configuring a new IPv6 address for an interface, enable address conflict detection on the interface. If a conflict address is detected, the device does not receive the IPv6 packet destined to the conflict address. This command is used to perform conflict detection again when the interval expires. If there is no conflict, the address can be used.	
Configuration Examples	The following example sets the interval for address conflict detection to 10s. FS(config)# ipv6 nd dad retry 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.13 ipv6 nd managed-config-flag

	Use this command to set the “managed address configuration” flag bit of the RA message. Use the no form of this command to restore the default setting.	
	ipv6 nd managed-config-flag	
	no ipv6 nd managed-config-flag	

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	This flag determines whether the host that receives the RA message obtains an IP address through stateful auto configuration. If the flag is set, the host obtains an IP address through stateful auto configuration, otherwise it does not be used.	
Configuration Examples	The following example set the “managed address configuration” flag bit of the RA message. FS(config-if)# ipv6 nd managed-config-flag	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd other-config-flag	Sets the flag for obtaining all information except IP address through stateful auto configuration.
Platform Description	N/A	

3.14 Ipv4 nd max-opt

	Use this command to set the maximum number of ND options. Use the no form of this command to restore the default setting.	
	ipv6 nd max-opt <i>value</i>	
	no ipv6 nd max-opt	
Parameter	Parameter	Description
Description	<i>value</i>	Sets the maximum number of ND options, in the range from 1 to 100.
Defaults	The default is 10.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to set the maximum number of ND options, such as source link layer address option, MTU option, redirection option and prefix option.	
Configuration Examples	The following example sets the maximum of ND options to 20. FS(config)# ipv6 nd max-opt 20	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.15 ipv6 nd ns-interval

	Use this command to set the interval for the interface to retransmitting NS (Neighbor Solicitation). Use the no form of this command to restore the default setting.	
	ipv6 nd ns-interval <i>milliseconds</i>	
	no ipv6 nd ns-interval	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	Interval for retransmitting NS in the range of 1000 to 429467295 milliseconds
Defaults	The default value in RA is 0 (unspecified); the interval for retransmitting NS is 1,000 milliseconds (1 second).	
Command mode	Interface configuration mode.	
Usage Guide	The configured value will be advertised through RA and will be used by the device itself. It is not recommended to set a too short interval.	
Configuration Examples	The following example sets the interval to 2,000 milliseconds, namely 2 seconds. FS(config-if)# ipv6 nd ns-interval 2000	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
Platform Description	N/A	

3.16 ipv6 nd other-config-flag

	Use this command to set "other stateful configuration" flag bit of the RA message. Use the no form of this command to delete the flag bit.	
	ipv6 nd other-config-flag	
	no ipv6 nd other-config-flag	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The flag bit is not set by default.	

Command mode	Interface configuration mode.	
Usage Guide	With this flag bit set, the flag bit of the RA message sent by the device is set. After receiving this flag bit, the host uses the dhcpv6 to acquire the information excluding the IPv6 address for the purpose of automatic configuration. When the managed address configuration is set, the default other stateful configuration is also set	
Configuration Examples	The following example sets "other stateful configuration" flag bit of the RA message. <pre>uijie(config-if-GigabitEthernet 0/1)# ipv6 nd other-config-flag</pre>	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
Platform Description	N/A	

3.17 ipv6 nd prefix

	Use this command to configure the address prefix included in the RA. Use the no form of this command to delete the set prefix or restore the default setting.	
	ipv6 nd prefix { <i>ipv6-prefix/prefix-length</i> default } [[<i>valid-lifetime preferred-lifetime</i>]] [at <i>valid-date preferred-date</i>] [infinite <i>preferred-lifetime</i>] [no-advertise] [[off-link] [no-autoconfig]]	
	no ipv6 nd prefix { <i>ipv6-prefix/prefix-length</i> default }	
Parameter Description	Parameter	Description
	<i>ipv6-prefix</i>	IPv6 network ID following the format defined in RFC4291
	<i>prefix-length</i>	Length of the IPv6 prefix. "/" shall be added in front of the prefix
	<i>valid-lifetime</i>	Valid lifetime of the RA prefix received by the host
	<i>preferred-lifetime</i>	Preferred lifetime of the RA prefix received by the host
	<i>at valid-date preferred-date</i>	Sets the dead line for the valid lifetime and that of the preferred lifetime, in day, month, year, hour, minute.
	infinite	Indicates that the prefix is always valid.
	default	Sets the default prefix.
	no-advertise	The prefix will not be advertised by the device.
	off-link	When the host sends an IPv6 packet, if the prefix of the destination address matches the set prefix, it is considered that the destination is on-link and is directly reachable. If this option is set, it indicates that the prefix is not used for on-link judgment.
	no-autoconfig	Indicates that the RA prefix received by the host cannot be used for auto address configuration.
Defaults	By default, the advertised prefix is the one set with ipv6 address on the interface. The default parameters of	

	the prefix configured in the RA are as follows: <i>valid-lifetime</i> : 2592000s (30 days) <i>preferred-lifetime</i> : 604800s (7 days), The prefix is advertised and is used for on-link judgment and auto address configuration.					
Command Mode	Interface configuration mode.					
Usage Guide	This command can be used to configure the parameters of each prefix, including whether to advertise the prefix. By default, the prefix advertised in RA is the one set with ipv6 address on the interface. To add other prefixes, use this command. ipv6 nd prefix default Set the default parameters to be used by the interface. If no parameter is specified for an added prefix, the parameters set with ipv6 nd prefix default will be used. Note that after a parameter is specified for the prefix, the default configuration will not be used. That is to say, the configuration of the prefix cannot be modified with ipv6 nd prefix default; only the prefix that uses all the default configurations can be modified with this command. at <i>valid-date preferred-date</i> The valid lifetime of a prefix can be specified in two ways. One way is to specify a fixed time for each prefix in the RA; the other way is to specify the end time (in this mode, the valid lifetime of the prefix sent in RA will be gradually reduced until the end time is 0).					
Configuration Examples	The following example adds a prefix for SVI 1. <pre>FS(config)# interface vlan 1 FS(config-if)# ipv6 nd prefix 2001::/64 infinite 2592000</pre> The following example sets the default prefix parameters for SVI 1 (they cannot be used for auto address configuration): <pre>FS(config)# interface vlan 1 FS(config-if)# ipv6 prefix default no-autoconfig</pre> If no parameter is specified, the default parameters will be used, and the prefix cannot be used for auto address configuration.					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ipv6 interface</td><td>Displays the RA information of an interface.</td></tr></table>	Command	Description	show ipv6 interface	Displays the RA information of an interface.	
Command	Description					
show ipv6 interface	Displays the RA information of an interface.					
Platform Description	N/A					

3.18 ipv6 nd ra-hoplimit

	Use this command to set the hopcount of the RA message. Use the no form of this command to restore the default setting.

	ipv6 nd ra-hoplimit <i>value</i>	
	no ipv6 nd ra-hoplimit	
Parameter	Parameter	Description
Description	<i>value</i>	Hopcount
Defaults	The default is 64.	
Command Mode	Interface configuration mode.	
Usage Guide	This command is used to set the hopcount of the RA message.	
Configuration Examples	The following example sets the hopcount to 110.	
	FS(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-interval	Sets the interval of sending the RA message.
	ipv6 nd ra-mtu	Sets the MTU of the RA message.
Platform Description	N/A	

3.19 ipv6 nd ra-interval

	Use this command to set the interval of sending the RA. Use the no form of this command to restore the default setting.	
	ipv6 nd ra-interval { <i>seconds</i> min-max <i>min_value</i> <i>max_value</i> }	
	no ipv6 nd ra-interval	
Parameter	Parameter	Description
Description	seconds	Interval of sending the RA message in seconds, 3-1800s.
	min-max	Maximum and minimum interval sending the RA message in seconds
	min_value	Minimum interval sending the RA message in seconds
	max_value	Maximum interval sending the RA message in seconds
Defaults	200s. The actual interval of sending the RA message will be fluctuated 20% based on 200s.	
Command Mode	Interface configuration mode.	

Usage Guide	If the device serves as the default device, the set interval shall not be longer than the lifetime of the device. Besides, to ensure other devices along the link occupies network bandwidth while sending the RA message, the actual interval for sending the RA message will be fluctuated 20% based on the set value. If the key word min-max is specified, the actual interval for sending the packet will be chosen between the range of minimum value and maximum value.	
Configuration Examples	The following example sets the interval to 110 seconds. FS(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval 110 The following example sets the interval to between 110 and 120 seconds. FS(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval min-max 110 120	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-hoplimit	Sets the hopfcount of the RA message.
	ipv6 nd ra-mtu	Sets the MTU of the RA message.
Platform Description	N/A	

3.20 ipv6 nd ra-lifetime

	Use this command to set the device lifetime of the RA sent on the interface. Use the no form of this command to restore the default setting.	
	ipv6 nd ra-lifetime <i>seconds</i>	
	no ipv6 nd ra-lifetime	
Parameter	Parameter	Description
Description	<i>seconds</i>	Default life time of the device on the interface, in the range from 0 to 9000 in the unit of seconds.
Defaults	The default is 1,800.	
Command Mode	Interface configuration mode.	
Usage Guide	The router lifetime field is available in each RA. It specifies the time during which the hosts along the link of the interface can select the device as the default device. If the value is set to 0, the device will not serve as the default device any longer. If it is not set to 0, it shall be larger than or equal to the interval of sending the RA (ra-interval)	
Configuration Examples	The following example sets the device lifetime to 2,000 seconds. FS(config-if-GigabitEthernet 0/1)# ipv6 nd ra-lifetime 2000	

Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-interval	Sets the interval of sending the RA.
	ipv6 nd ra-hoplimit	Sets the hopcount of the RA.
	ipv6 nd ra-mtu	Sets the MTU of the RA.
Platform Description	N/A	

3.21 ipv6 nd ra-mtu

	Use this command to set the MTU of the RA message. Use the no form of this command to restore the default setting.	
	ipv6 nd ra-mtu <i>value</i>	
	no ipv6 nd ra-mtu	
Parameter Description	Parameter	Description
	<i>value</i>	MTU value, in the range from 0 to 4294967295.
Defaults	IPv6 MTU value of the network interface.	
Command Mode	Interface configuration mode.	
Usage Guide	If it is specified as 0, the RA will not have the MTU option	
Configuration Examples	The following example sets the MTU to 1,4000 bytes.	
	FS(config-if)# ipv6 nd ra-mtu 1400	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
	ipv6 nd ra-lifetime	Sets the lifetime of the device.
	ipv6 nd ra-interval	Sets the interval of sending the RA message.
	ipv6 nd ra-hoplimit	Sets the hopcount of the RA message.
Platform Description	N/A	

3.22 ipv6 nd reachable-time

	Use this command to set the reachable time after the interface checks the reachability of the neighbor dynamically learned through NDP. Use the no form of this command to restore the default setting.	
	ipv6 nd reachable-time <i>milliseconds</i>	
	no ipv6 nd reachable-time	

Parameter	Parameter	Description
Description	<i>milliseconds</i>	Reachable time for the neighbor in the range from 0 to 3,600,000 in the unit of milliseconds.
Defaults	The default value in RA is 0 (unspecified); the reachable time for the neighbor is 30,000 milliseconds (30 seconds) when the device discovers the neighbor.	
Command Mode	Interface configuration mode.	
Usage Guide	The device checks the unreachable neighbor through the set time. A shorter time means that the device can check the neighbor failure more quickly, but more network bandwidth and device resource will be occupied. Therefore, it is not recommended to set a too short reachable time. The configured value will be advertised through RA and will be used by the device itself. If the value is set to 0, it indicates that the time is not specified, that is, the default value is used.	
Configuration Examples	The following example sets the reachable time to 1,000,000 milliseconds, namely 1,000 seconds. <pre>FS(config-if-GigabitEthernet 0/1)# ipv6 nd reachable-time 1000000</pre>	
Related Commands	Command	Description
Commands	show ipv6 interface	Displays the interface information.
Platform	N/A	
Description		

3.23 ipv6 nd resolve vlan

	Use this command to enable active sending of NS resolution requests to a specific sub VLAN of a super VLAN. Use the no form of this command to disable the active sending of NS resolution requests to a specific sub VLAN of a super VLAN. Use the default form of this command to restore the default settings. <code>ipv6 nd resolve vlan {vlan-list none}</code> <code>no ipv6 nd resolve vlan {vlan-list none}</code>	
	default ipv6 nd resolve vlan	
Parameter	Parameter	Description
Description	<i>vlan-list</i>	Sets the list of sub VLANs in a super VLAN, where NS resolution requests are sent only to these sub VLANs.
	none	Specifies that no NS resolution request is sent to any sub VLAN of a super VLAN.
Defaults	The function is disabled by default.	
Command Mode	Global configuration mode	

Default Level	2
Usage Guide	If many sub VLANs exist in a super VLAN, when the device sends NS resolution requests to learn ND entries of the peer, the NS resolution requests are sent to the entire super VLAN by default. In this case, too many sub VLANs may cause a great number of packet replications, and therefore affect device performance. Most STAs (such as PCs and servers) request information about ND neighbors from the gateway before accessing the network. Therefore, it is unnecessary to actively broadcast NS resolution requests to the sub VLANs where these STAs reside. For dumb terminals that do not actively send NA advertisements, run the <code>ipv6 nd resolve vlan <i>vlan-list</i></code> command to resolve and send ND entries to VLANs in the specified VLAN list.  After the <code>ipv6 ns resolve vlan <i>vlan-list</i></code> command is configured, NS resolution requests are sent only to VLANs in the VLAN list of a super VLAN. It should be particularly noted that if authentication-free VLANs are configured but not included in the VLAN list specified in the <code>ipv6 nd resolve vlan</code> command, NS resolution requests are not broadcast to the authentication-free VLANs.
Configuration Examples	The following example enables the device to provide active NS resolution for VLANs 10–20 and VLANs 25–30. <pre>FS(config)# ipv6 nd resolve vlan 10-20, 25-30</pre> The following example removes active NS resolution of VLANs 10–20. <pre>FS(config)# no ipv6 nd resolve vlan 10-20</pre> The following example configures the device not to provide active NS resolution for any sub VLAN of a super VLAN. <pre>FS(config)# ipv6 nd resolve vlan none</pre>
Verification	Run the <code>show running-config</code> command to display configurations.

3.24 ipv6 nd state-time

	Use this command to set the period for the neighbor to maintain the state. Use the no form of this command to restore the default setting.					
	ipv6 nd stale-time <i>seconds</i>					
	no ipv6 nd stale-time					
Parameter Description	<table><tr><th>Parameter</th><th>Description</th></tr><tr><td><i>Seconds</i></td><td>Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.</td></tr></table>	Parameter	Description	<i>Seconds</i>	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.	
Parameter	Description					
<i>Seconds</i>	Sets the period for the neighbor to maintain the state, in the range from 0 to 86400 in the unit of seconds.					
Defaults	The default is 3600.					
Command Mode	Global configuration mode					
Usage Guide	This command is used to set the period for the neighbor to maintain the state. After the period expires, neighbor unreachability detection is performed. The shorter the period, the faster the neighbor is found unreachable. On the other hand, more network bandwidth and device resources are consumed. Therefore, it is recommended to set a value not too small.					

Configuration Examples	The following example sets the period to 600 seconds for the neighbor to maintain the state. FS(config)# ipv6 nd stale-time 600	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.25 ipv6 nd suppress-auth-vlan-ns

	Use this command to disable the SVI interface from sending the NS packet to the authentication VLAN. Use the no form of this command to disable this function.	
	ipv6 nd suppress-auth-vlan-ns	
	no ipv6 nd suppress-auth-vlan-ns	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is supported on the SVI interface in gateway authentication mode.	
Configuration Examples	The following example enables VLAN 2 to send the NS packet to the authentication VLAN. FS(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.26 ipv6 nd suppress-ra

	Use this command to disable the interface from sending the RA message. Use the no form of this command to enable the function.	
	ipv6 nd suppress-ra	
	no ipv6 nd suppress-ra	

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The ipv6 nd suppress-ra command is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	This command suppresses the sending of the RA message on an interface.	
Configuration Examples	The following example disables the interface from sending the RA message.	
	FS(config-if-GigabitEthernet 0/1)# ipv6 nd suppress-ra	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
Platform Description	N/A	

3.27 ipv6 nd unresolved

	Use this command to set the maximum number of the unresolved neighbor table entries. Use the no form of this command to restore the default setting.	
	ipv6 nd unresolved <i>number</i>	
	no ipv6 nd unresolved	
Parameter Description	Parameter	Description
	<i>number</i>	Sets the maximum number of the unresolved neighbor table entries, in the range from 1 to the neighbor table size supported by the device.
Defaults	The default is 0. (The maximum number is the neighbor table size supported by the device)	
Command Mode	Global configuration mode	
Usage Guide	This command is used to prevent unresolved ND table entries generated by malicious scan attacks from consuming table entry resources,	
Configuration Examples	The following example sets the maximum number of the unresolved neighbor table entries to 200. FS(config)# ipv6 nd unresolved 200	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

3.28 ipv6 neighbor

	Use this command to configure a static neighbor. Use the no form of this command to delete a static neighbor.	
	ipv6 neighbor <i>ipv6-address interface-id hardware-address</i>	
	no ipv6 neighbor <i>ipv6-address interface-id</i>	
Parameter	Parameter	Description
Description	<i>ipv6-address</i>	The neighbor IPv6 address, in the form as defined in RFC4291.
	<i>interface-id</i>	Specifies the network interface where the neighbor is (including Router Port, L3 AP port and SVI interface).
	<i>hardware-address</i>	The 48-bit MAC address, a dotted triple of four-digit hexadecimal numbers.
Defaults	No static neighbor is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	This command can only be configured on the interface enabled with IPv6 protocol, similar to the ARP command. If the neighbor to be configured has been learned through Neighbor Discovery Protocol (NDP) and stored in the NDP neighbor table, the dynamic neighbor turns to be static. If the static neighbor is valid, it is always reachable. An invalid static neighbor refers to the neighbor whose IPv6 address is not valid (not in the IPv6 network segment configured for the interface or interface address conflict). The packet is not forwarded to the MAC address as specified by the invalid static neighbor. The invalid static neighbor is in inactive state. Use the <code>show ipv6 neighbor static</code> command to display the state of the static neighbor. Use the clear ipv6 neighbors command to clear all neighbors learned dynamically through NDP.	
Configuration Examples	The following example configures a static neighbor on SVI 1. <pre>FS(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

3.29 ipv6 ns-linklocal-src

	Use this command to set the local address of the link as the source IP address to send neighbor requests. Use the no form of this command to use the global IP address w as the source address to send neighbor requests.	
	ipv6 ns-linklocal-src	
	no ipv6 ns-linklocal-src	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The local address of the link is always used as the source address to send neighbor requests.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the local address of the link as the source IP address to send neighbor requests.	
	FS(config)# no ipv6 ns-linklocal-src	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.30 ipv6 redirects

	Use this command to control whether to send ICMPv6 redirect message when the switch receives and forwards an IPv6 packet through an interface. Use the no form of this command to restore the default setting.	
	ipv6 redirects	
	no ipv6 redirects	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	The transmission rate of any ICMPv6 error message is limited. By default, it is 10pps.	
Configuration	The following example enables ICMPv6 redirection on interface GigabitEthernet 0/1.	

Examples	FS(config-if-GigabitEthernet 0/1)# ipv6 redirects	
Related Commands	Command	Description
	show ipv6 interface	Displays the interface information.
Platform Description	N/A	

3.31 ipv6 source-route

	Use this command to forward the IPv6 packet with route header. Use the no form of this command to restore the default setting.	
	ipv6 source-route	
	no ipv6 source-route	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The ipv6 source-route command is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	Because of the potential security of the header of type 0 route, it's easy for the device to suffer from the denial service attack. Therefore, forwarding the IPv6 packet with route header is disabled by default. However, the IPv6 packet of route header with type 0 that destined to the local machine is processed.	
Configuration Examples	The following example forwards the IPv6 packet with route header. FS(config)# no ipv6 source-route	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.32 show ipv6 address

	Use this command to display the IPv6 addresses.	
	show ipv6 address [<i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name

Defaults	N/A					
Command Mode	Privileged EXEC mode.					
Usage Guide	N/A					
Configuration Examples	The following example displays all IPv6 address configured on the device. <pre>FS#show ipv6 addr Global unicast address limit: 1024, Global unicast address count: 2 Tentative address count: 3,Duplicate address count: 0 Preferred address count: 0,Deprecated address count: 0 GigabitEthernet 0/5 2003::1::23/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE fe80::2d0:f8ff:febf:deb2/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE 2005::1::1111/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE FS#</pre> The following example displays the IPv6 address configured on the GigabitEthernet 0/1. <pre>FS#show ipv6 addr gi 0/5 Global unicast address count: 2 Tentative address count: 3,Duplicate address count: 0 Preferred address count: 0,Deprecated address count: 0 2003::1::23/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE fe80::2d0:f8ff:febf:deb2/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE 2005::1::1111/64 Tentative Preferred lifetime: INFINITE, Valid lifetime: INFINITE FS#</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

3.33 show ipv6 general-prefix

	Use this command to display the information of the general prefix.
	show ipv6 general-prefix

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	Use this command to display the information of the general prefix including the manually configured and learned from the DHCPv6 agent.	
Configuration Examples	The following example displays the information of the general prefix. <pre>FS# show ipv6 general-prefix</pre> There is 1 general prefix. IPv6 general prefix my-prefix, acquired via Manual configuration <pre>2001:1111:2222::/48 2001:1111:3333::/48</pre>	
Related Commands	Command	Description
	ipv6 general-prefix	Configures the general prefix.
Platform Description	N/A	

3.34 show ipv6 interface

	Use this command to display the IPv6 interface information.	
	show ipv6 interface [<i>interface-id</i>] [<i>ra-info</i>] [<i>brief</i> [<i>interface-id</i>]]	
Parameter	Parameter	Description
Description	interface-id	Interface (including Ethernet interface, aggregate port, or SVI)
	ra-info	Displays the RA information of the interface.
	brief	Displays the brief information of the interface (interface status and address information).
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	Use this command to display the address configuration, ND configuration and other information of an IPv6 interface.	
Configuration	The following example displays the information of the IPv6 interface.	

Examples

```

FS# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND device advertisements live for 1800 seconds

```

The following line is included in the above information: 2001::1, subnet is 2001::/64 **[TENTATIVE]**. The flag bit in the [] following the INET6 address is explained as follows:

Flag	Meaning
ANYCAST	Indicate that the address is an anycast address.
TENTATIVE	Indicate that the DAD is underway. The address is a tentative before the DAD is completed.
DUPLICATED	Indicate that a duplicate address exists.
DEPRECATED	Indicate that the preferred lifetime of the address expires.
NODAD	Indicate that no DAD is implemented for the address.
AUTOIFID	Indicate that the interface ID of the address is automatically generated by the system, which is usually an EUI-64 ID.
PRE	Indicate the IP stateless address that is automatically configured.
GEN	Indicate the IP address that is generated by the general prefix.

The following example displays the RA information of the IPv6 interface.

```
FS# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND device advertisements live for 1800 seconds
ND device advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def,Auto,vltime: 2592000, pltime: 604800, flags: LA)
```

Description of the fields in **ra-info**:

Field	Meaning
RA timer is stopped (on)	Indicate whether the RA timer is started.
waits	Indicate that the RS is received but the number of the responses is not available.
initcount	Indicate the number of the RAs when the RA timer is restarted.
RA(out/in/ inconsistent)	out: Indicate the number of the RAs that are sent. In: Indicate the number of the RAs that are received. inconsistent: Indicate the number of the received RAs in which the parameters are different from those contained in the RAs advertised by the device.
RS(input)	Indicate the number of the RSs that are received.
Link-layer address	Link-layer address of the interface.
Physical MTU	Link MTU of the interface.
!M M	!M indicates the managed-config-flag bit in the RA is not set. M: Conversely
!O O	!O indicates the other-config-flag bit in the RA is not set. O: Conversely

Description of the fields of the prefix list in **ra-info**:

	Field	Meaning
	total	The number of the prefixes of the interface.
	fec0:1:1:1::/64	A specific prefix.
	Def	Indicate that the interfaces use the default prefix.
	Auto CFG	Auto: Indicate the prefix is automatically generated after the interface is configured with the corresponding IPv6 address. CFG: Indicate that the prefix is manually configured.
	!Adv	Indicate that the prefix will not be advertised.
	vlttime	Valid lifetime of the prefix, measured in seconds.
	pltime	Preferred lifetime of the prefix, measured in seconds.
	L !L	L: Indicate that the on-link in the prefix is set. !L: Indicate that the on-link in the prefix is not set.
	A !A	A: Indicate that the auto-configure in the prefix is set. !A: It indicates that the auto-configure in the prefix is not set.
The following example displays the brief information of the IPv6 interface.		
<pre>FS#show ipv6 interface brief GigabitEthernet 0/1 [down/down] 2222::2 FE80::1614:4BFF:FE5C:ED3A</pre>		
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.35 show ipv6 neighbors

	Use this command to display the IPv6 neighbors.	
	show ipv6 neighbors [vrf <i>vrf-name</i>] [verbose] [<i>interface-id</i>] [<i>ipv6-address</i>] [static] [oob]	
Parameter Description	Parameter	Description
	verbose	Displays the neighbor details.
	static	Displays the validity status of static neighbors.
	<i>vrf-name</i>	VRF name
	<i>interface-id</i>	Displays the neighbors of the specified interface.
	<i>ipv6-address</i>	Displays the neighbors of the specified IPv6 address.
	oob	Displays the IPv6 neighbors of the MGMT port.

Defaults	N/A										
Command Mode	Privileged EXEC mode.										
Usage Guide	N/A										
Configuration Examples	The following example displays the neighbors on the SVI 1 interface. <pre>FS# show ipv6 neighbors vlan 1 IPv6 Address Linklayer Addr Interface fa::1 00d0.0000.0002 vlan 1 fe80::200:ff:fe00:2 00d0.0000.0002 vlan 1</pre> The following example displays the neighbor details. <pre>FS# show ipv6 neighbors verbose IPv6 Address Linklayer Addr Interface 2001::1 00d0.f800.0001 vlan 1 State: Reach/H Age: - asked: 0 fe80::200:ff:fe00:1 00d0.f800.0001 vlan 1 State: Reach/H Age: - asked: 0</pre> <table border="1"> <thead> <tr> <th>Field</th><th>Meaning</th></tr> </thead> <tbody> <tr> <td>IPv6 Address</td><td>IPv6 address of the Neighbor</td></tr> <tr> <td>Linklayer Addr</td><td>Link address, namely, MAC address. If it is not available, incomplete is displayed.</td></tr> <tr> <td>Interface</td><td>Interface the neighbor locates.</td></tr> <tr> <td>State</td><td> State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3). </td></tr> </tbody> </table>	Field	Meaning	IPv6 Address	IPv6 address of the Neighbor	Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.	Interface	Interface the neighbor locates.	State	State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3).
Field	Meaning										
IPv6 Address	IPv6 address of the Neighbor										
Linklayer Addr	Link address, namely, MAC address. If it is not available, incomplete is displayed.										
Interface	Interface the neighbor locates.										
State	State of the neighbor: state/H(R) The values of STATE are as below: INCMP (Incomplete): The address resolution of the neighbor is underway, the NS is sent, but the NA is not received. REACH (Reachable): The switch is connected with the neighbor. In this state, the switch takes no additional action when sending packets to the neighbor. STALE: The reachable time of the neighbor expires. In this state, the switch takes no additional action; it only starts NUD (Neighbor Unreachability Detection) after a packet is sent to the neighbor. DELAY: A packet is sent to the neighbor in STALE state. If the STALE state changes to DELAY, DELAY will be changed to PROBE if no neighbor reachability notification is received within DELAY_FIRST_PROBE_TIME seconds (5s), the NS will be sent to the neighbor to start NUD. PROBE: The NUD is started to check the reachability of the neighbor. The NS packets are sent to the neighbor at the interval of RetransTimer milliseconds until the response from the neighbor is received or the number of the sent NSs hits MAX_UNICAST_SOLICIT(3).										

		?: Unknown state. /R—indicate the neighbor is considered as a device /H: The neighbor is a host.												
	Age	The reachable time of the neighbor. '-' indicates that the neighbor is always reachable. Note that the reachability of a static neighbor depends on the actual situation. 'expired' indicates that the lifetime of the neighbor expires, and the neighbor is waits for the triggering of NUD.												
	Asked	The number of the NSs that are sent to the neighbor for the resolution of the link address of the neighbor.												
	The following example displays the status of static neighbors. FS# show ipv6 neighbors static													
	<table><tr><td>IPv6 Address</td><td>Linklayer Addr</td><td>Interface</td><td>State</td></tr><tr><td>2001:1::1</td><td>00d0.f822.33ab</td><td>GigabitEthernet 0/14</td><td>ACTIVE</td></tr><tr><td>2001:2::2</td><td>00d0.f822.33ac</td><td>VLAN 1</td><td>INACTIVE</td></tr></table>		IPv6 Address	Linklayer Addr	Interface	State	2001:1::1	00d0.f822.33ab	GigabitEthernet 0/14	ACTIVE	2001:2::2	00d0.f822.33ac	VLAN 1	INACTIVE
IPv6 Address	Linklayer Addr	Interface	State											
2001:1::1	00d0.f822.33ab	GigabitEthernet 0/14	ACTIVE											
2001:2::2	00d0.f822.33ac	VLAN 1	INACTIVE											
Related Commands	Command	Description												
	ipv6 neighbor	Configures a neighbor.												
Platform Description	N/A													

3.36 show ipv6 neighbors statistics

	Use the following commands to display the statistics of one IPv6 neighbors.	
	show ipv6 neighbors [vrf vrf-name] statistics	
Parameter Description	Parameter	Description
	vrf-name	VRF name
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistics of the global neighbors. <pre>FS#show ipv6 neighbor statistics</pre> <pre>Memory: 0 bytes Entries: 0 Static: 0,Dynamic: 0,Local: 0 Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0 FS#</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	Supported on all platforms.	

3.37 show ipv6 neighbor statistics per-mac

	Use this command to display the number of neighbor entries of every MAC address.	
	show ipv6 neighbor statistics per-mac [<i>interface-name</i>] [<i>mac-address</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface ID
	<i>mac-address</i>	MAC address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the number of neighbor entries of every MAC address..	
	FS# show ipv6 neighbor statistics per-mac	
	Interface MAC address Statistics	

	VLAN 1 0000:0000:0001 3	
	VLAN 1 0000:0000:0002 5	
	VLAN 2 0000:0000:0003 10	
	Field	Description
	Interface	Interface ID.
	MAC address	MAC address.
	Statistics	ND entry number.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.38 show ipv6 packet statistics

	Use this command to display the statistics of IPv6 packets.
	show ipv6 packet statistics [<i>total</i> <i>interface-name</i>]

Parameter	Parameter	Description
Description	total	Displays total statistics of all interfaces.
	interface-name	Interface name
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the total statistics of the Ipv6 packets and the statistics of each interface. <pre> FS#show ipv6 pack statistics Total Received 0 packets, 0 bytes Unicast:0,Multicast:0 Discards:0 HdrErrors:0(HoplimitExceeded:0,Others:0) NoRoutes:0 Others:0 Sent 0 packets, 0 bytes Unicast:0,Multicast:0 GigabitEthernet 0/5 Received 0 packets, 0 bytes Unicast:0,Multicast:0 Discards:0 HdrErrors:0(HoplimitExceeded:0,Others:0) NoRoutes:0 Others:0 Sent 0 packets, 0 bytes Unicast:0,Multicast:0 FS# </pre> The following example displays the total statistics of the Ipv6 packets. <pre> FS#show ipv6 pack statistics total Total Received 0 packets, 0 bytes Unicast:0,Multicast:0 Discards:0 HdrErrors:0(HoplimitExceeded:0,Others:0) NoRoutes:0 Others:0 Sent 0 packets, 0 bytes </pre>	

	Unicast:0,Multicast:0	
	FS#	
Related Commands	Command	Description
	N/A	N/A
Platform Description	Supported on all platforms.	

3.39 show ipv6 raw-socket

	Use this command to display all original IPv6 sockets.	
	show ipv6 raw-socket [<i>num</i>]	
Parameter Description	Parameter	Description
	<i>num</i>	Protocol number
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays all original IPv6 sockets.	
	FS# show ipv6 raw-socket	
	Number Protocol Process name	
	1 ICMPv6 vrrp.elf	
	2 ICMPv6 tcpip.elf	
	3 VRRP vrrp.elf	
	Total: 3	
	Field	Description
	Number	Number.
	Process name	Process name.
	Protocol	Protocol number
	Total	Total number of sockets.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.40 show ipv6 routers

	In the IPv6 network, some neighbor routers send out the advertisement messages. Use this command to display the neighbor routers and the advertisement.	
	show ipv6 routers [<i>interface-type interface-number</i>]	
Parameter	Parameter	Description
Description	<i>interface-type interface-number</i>	(Optional) Displays the routing advertisement of the specified interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	Use this command to display the neighbor routers and the routing advertisement. If no interface is specified, all the routing advertisement of this device will be displayed.	
Configuration Examples	The following example displays the IPv6 router <pre> FS# show ipv6 routers Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500 Preference=MEDIUM Reachable time 0 msec, Retransmit time 0 msec Prefix 6001:3::/64 onlink autoconfig Valid lifetime 2592000 sec, preferred lifetime 604800 sec Prefix 6001:2::/64 onlink autoconfig Valid lifetime 2592000 sec, preferred lifetime 604800 sec </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.41 show ipv6 sockets

	Use this command to display all IPv6 sockets.	
	show ipv6 sockets	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode.																																																																																							
Usage Guide	N/A																																																																																							
Configuration Examples	The following example displays all IPv6 sockets. FS# show ipv6 sockets <table><thead><tr><th>Number</th><th>Process name</th><th>Type</th><th>Protocol</th><th>LocalIP:Port</th><th>ForeignIP:Port</th><th>State</th></tr></thead><tbody><tr><td>1</td><td>vrp.elf</td><td>RAW</td><td>ICMPv6</td><td>:::58</td><td>:::0</td><td>*</td></tr><tr><td>2</td><td>tcpip.elf</td><td>RAW</td><td>ICMPv6</td><td>:::58</td><td>:::0</td><td>*</td></tr><tr><td>3</td><td>vrp.elf</td><td>RAW</td><td>VRRP</td><td>:::112</td><td>:::0</td><td>*</td></tr><tr><td>4</td><td>snmpd</td><td>DGRAM</td><td>UDP</td><td>:::161</td><td>:::0</td><td>*</td></tr><tr><td>5</td><td>snmpd</td><td>DGRAM</td><td>UDP</td><td>:::162</td><td>:::0</td><td>*</td></tr><tr><td>6</td><td>dhcp6.elf</td><td>DGRAM</td><td>UDP</td><td>:::547</td><td>:::0</td><td>*</td></tr><tr><td>7</td><td>sshd</td><td>STREAM</td><td>TCP</td><td>:::22</td><td>:::0</td><td>LISTEN</td></tr><tr><td>8</td><td>telnetd</td><td>STREAM</td><td>TCP</td><td>:::23</td><td>:::0</td><td>LISTEN</td></tr></tbody></table> Total: 8 <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Number</td><td>Number.</td></tr><tr><td>Process name</td><td>Process name.</td></tr><tr><td>Type</td><td>Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.</td></tr><tr><td>Protocol</td><td>Protocol number</td></tr><tr><td>LocalIP:Port</td><td>Local IPv6 address and port.</td></tr><tr><td>ForeignIP:Port</td><td>Peer IPv6 address and port.</td></tr><tr><td>State</td><td>State (for IPv6 TCP sockets).</td></tr><tr><td>Total</td><td>Total number of sockets.</td></tr></tbody></table>							Number	Process name	Type	Protocol	LocalIP:Port	ForeignIP:Port	State	1	vrp.elf	RAW	ICMPv6	:::58	:::0	*	2	tcpip.elf	RAW	ICMPv6	:::58	:::0	*	3	vrp.elf	RAW	VRRP	:::112	:::0	*	4	snmpd	DGRAM	UDP	:::161	:::0	*	5	snmpd	DGRAM	UDP	:::162	:::0	*	6	dhcp6.elf	DGRAM	UDP	:::547	:::0	*	7	sshd	STREAM	TCP	:::22	:::0	LISTEN	8	telnetd	STREAM	TCP	:::23	:::0	LISTEN	Field	Description	Number	Number.	Process name	Process name.	Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.	Protocol	Protocol number	LocalIP:Port	Local IPv6 address and port.	ForeignIP:Port	Peer IPv6 address and port.	State	State (for IPv6 TCP sockets).	Total	Total number of sockets.
Number	Process name	Type	Protocol	LocalIP:Port	ForeignIP:Port	State																																																																																		
1	vrp.elf	RAW	ICMPv6	:::58	:::0	*																																																																																		
2	tcpip.elf	RAW	ICMPv6	:::58	:::0	*																																																																																		
3	vrp.elf	RAW	VRRP	:::112	:::0	*																																																																																		
4	snmpd	DGRAM	UDP	:::161	:::0	*																																																																																		
5	snmpd	DGRAM	UDP	:::162	:::0	*																																																																																		
6	dhcp6.elf	DGRAM	UDP	:::547	:::0	*																																																																																		
7	sshd	STREAM	TCP	:::22	:::0	LISTEN																																																																																		
8	telnetd	STREAM	TCP	:::23	:::0	LISTEN																																																																																		
Field	Description																																																																																							
Number	Number.																																																																																							
Process name	Process name.																																																																																							
Type	Socket type. RAW indicates the raw socket. DGRAM indicates data packet type. STREAM indicates traffic type.																																																																																							
Protocol	Protocol number																																																																																							
LocalIP:Port	Local IPv6 address and port.																																																																																							
ForeignIP:Port	Peer IPv6 address and port.																																																																																							
State	State (for IPv6 TCP sockets).																																																																																							
Total	Total number of sockets.																																																																																							
Related Commands	Command			Description																																																																																				
	N/A			N/A																																																																																				
Platform Description	N/A																																																																																							

3.42 show ipv6 udp

	Use this command to display all IPv6 UDP sockets.
	show ipv6 udp [local-port num] [peer-port num]
	Use this command to display IPv6 UDP socket statistics.
	show ipv6 udp statistics

Parameter	Parameter	Description																										
Description	local-port <i>num</i>	Local port number.																										
	peer-port <i>num</i>	Peer port number.																										
Defaults	N/A																											
Command Mode	Privileged EXEC mode																											
Usage Guide	N/A																											
Configuration Examples	The following example displays all IPv6 UDP sockets. FS# show ipv6 udp <table><thead><tr><th>Number</th><th>Local Address</th><th>Peer Address</th><th>Process name</th></tr></thead><tbody><tr><td>1</td><td>:::161</td><td>:::0</td><td>snmpd</td></tr><tr><td>2</td><td>:::162</td><td>:::0</td><td>snmpd</td></tr><tr><td>3</td><td>:::547</td><td>:::0</td><td>dhcp6.elf</td></tr></tbody></table> <table><thead><tr><th>Filed</th><th>Description</th></tr></thead><tbody><tr><td>Number</td><td>Number.</td></tr><tr><td>Local Address</td><td>Local IPv6 address and port.</td></tr><tr><td>Peer Address</td><td>Peer IPv6 address and port.</td></tr><tr><td>Process name</td><td>Process name.</td></tr></tbody></table>		Number	Local Address	Peer Address	Process name	1	:::161	:::0	snmpd	2	:::162	:::0	snmpd	3	:::547	:::0	dhcp6.elf	Filed	Description	Number	Number.	Local Address	Local IPv6 address and port.	Peer Address	Peer IPv6 address and port.	Process name	Process name.
Number	Local Address	Peer Address	Process name																									
1	:::161	:::0	snmpd																									
2	:::162	:::0	snmpd																									
3	:::547	:::0	dhcp6.elf																									
Filed	Description																											
Number	Number.																											
Local Address	Local IPv6 address and port.																											
Peer Address	Peer IPv6 address and port.																											
Process name	Process name.																											
Related Commands	Command	Description																										
	N/A	N/A																										
Platform Description	N/A																											

4 DHCP Commands

4.1 address range

	Use this command to specify the network segment range of the addresses that can be allocated by CLASS associated with DHCP address pool. Use the no form of this command to restore the default setting.	
	address range <i>low-ip-address high-ip-address</i>	
	no address range	
Parameter	Parameter	Description
Description	low-ip-address	Start address in the network segment range.
	high-ip-address	End address in the network segment range.
Defaults	By default, the associated CLASS is not configured with the network segment range. The default is the address pool range.	
Command Mode	Address pool CLASS configuration mode.	
Usage Guide	Each CLASS corresponds to one network range which must be from low address to high address, so as to allow the duplication of network segment range between multiple CLASSes. If the CLASS associated with the address pool is specified without configuring the corresponding network segment range, the default network segment range of this CLASS is same as the range of the address pool where this CLASS is.	
Configuration Examples	The following example configures the network segment of class1 associated with address pool mypool0 ranging from 172.16.1.1 to 172.16.1.8. <pre>FS(config)# ip dhcp pool mypool0 FS(dhcp-config)# class class1 FS (config-dhcp-pool-class)# address range 172.16.1.1 172.16.1.8</pre>	
Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
	class	Configures the CLASS associated with the DHCP address pool and enters the address pool CLASS configuration mode.
Platform Description	N/A	

4.2 address-manage

	Use this command to enter the AM rule configuration mode.
	address-manage

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is configured on the DHCP server and used in combination with Super VLAN.	
Configuration Examples	The following example enters the AM rule configuration mode. FS(config)#address-manage	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.3 bootfile

Use this command to define the startup mapping file name of the DHCP client. Use the **no** or **default** form of this command to restore the default setting.

bootfile *file-name*

no bootfile

default bootfile

Parameter	Parameter	Description
Description	<i>file-name</i>	Startup file name.

Defaults No startup file name is defined by default.

Command Mode DHCP address pool configuration mode

Usage Guide Some DHCP clients need to download the operating system and configure the file during the startup. The DHCP server should provide the mapping file name required for the startup, so that DHCP clients can download the file from the corresponding server (such as TFTP). Other servers are defined by the **next-server** command.

Configuration Examples The following example defines the device.conf as the startup file name.
 bootfile device.conf

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	next-server	Configures the next server IP address of the DHCP client startup process.

Platform N/A

Description

4.4 class

	Use this command to configure the associated CLASS in the DHCP address pool. Use the no form of this command to restore the default setting.	
	class <i>class-name</i>	
	no class	
Parameter Description	Parameter	Description
	<i>class-name</i>	Class name, which can be the character string or numeric such as myclass or 1.
Defaults	By default, no CLASS is associated with the address pool.	
Command Mode	DHCP address pool configuration mode	
Usage Guide	Each DHCP address pool performs the address assignment according to the Option82 matching information. We can divide this Option82 information into classes and specify the available network segment range for these classes in the DHCP address pool. These classes are called CLASS. One DHCP address pool can map to multiple CLASSES, and each CLASS can specify different network segment range. During the address assignment, firstly, ensure the assignable address pool through the network segment where the client is, then according to the Option82 information further ensure the CLASS and assign the IP address from the network segment range corresponding to the CLASS. If one request packet matches multiple CLASSES in the address pool, perform the address assignment according to the sequencing of configuring the CLASS in the address pool. If this CLASS's assigned addresses have been to the upper limit, then continue to assign the address from the next CLASS, and so on. Each CLASS corresponds to one network segment range that must be from low addresses to high addresses and the duplicated network ranges between multiple CLASSES are allowed. If the CLASS corresponding to the address pool is specified and the network segment corresponding to the CLASS is not configured, this CLASS's default network segment range is same as the range of address pool where the CLASS is.	
Configuration Examples	The following example configures the address <i>mypool0</i> to associate with class1. <pre>FS(config)# ip dhcp pool mypool0 FS(dhcp-config)# class class1</pre>	
Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool

		configuration mode.
Platform	N/A	
Description		

4.5 clear ip dhcp binding

	Use this command to clear the DHCP binding table in the privileged user mode.	
	clear ip dhcp binding { * <i>ip-address</i> }	
Parameter	Parameter	Description
Description	*	Deletes all DHCP bindings.
	<i>ip-address</i>	Deletes the binding of the specified IP addresses.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command can only clear the automatic DHCP binding, but the manual DHCP binding can be deleted by the no ip dhcp pool command.	
Configuration Examples	The following example clears the DHCP binding with the IP address 192.168.12.100. clear ip dhcp binding 192.168.12.100	
Related Commands	Command	Description
	show ip dhcp binding	Displays the address binding of the DHCP server.
Platform	N/A	
Description		

4.6 clear ip dhcp conflict

	Use this command to clear the DHCP address conflict record.	
	clear ip dhcp conflict { * <i>ip-address</i> }	
Parameter	Parameter	Description
Description	*	Deletes all DHCP address conflict records.
	<i>ip-address</i>	Deletes the conflict record of the specified IP addresses.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	

Usage Guide	The DHCP server uses the ping session to detect the address conflict, while the DHCP client uses the address resolution protocol (ARP) to detect the address conflict. The clear ip dhcp conflict command can be used to delete the history conflict record.	
Configuration Examples	The following example clears all address conflict records. <code>clear ip dhcp conflict *</code>	
Related Commands	Command	Description
	ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.
	show ip dhcp conflict	Displays the address conflict that the DHCP server detects when it assigns an IP address.
Platform Description	N/A	

4.7 clear ip dhcp history

	Use this command to clear the address assigned by the DHCP server.	
	clear ip dhcp history { * <i>mac-address</i> }	
Parameter Description	Parameter	Description
	*	Clears all addresses assigned by the DHCP server.
	<i>mac-address</i>	Clears the address assigned by the DHCP server corresponding to the specified MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is configured on the DHCP server.	
Configuration Examples	The following example clears all addresses assigned by the DHCP server. <code>FS# clear ip dhcp history *</code>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.8 clear ip dhcp server detect

	Use this command to clear statistics about the fake DHCP server.	
	clear ip dhcp server detect { * <i>ip-address</i> }	
Parameter	Parameter	Description
Description	*	Clears statistics about all fake DHCP servers.
	<i>ip-address</i>	Clears statistics about the specified fake DHCP server.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	The detected fake DHCP server addresses are saved on the server. You can use the clear ip dhcp server detect command to clear statistics about the fake DHCP server.	
Configuration Examples	The following example clears statistics about all fake DHCP servers. FS#clear ip dhcp server detect *	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.9 clear ip dhcp server rate

	Use this command to clear statistics about the packet processing rate of every module.	
	clear ip dhcp server rate	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear statistics about the packet processing rate of every module, including arp, hot backup, lsm, and socket.	
Configuration Examples	The following example clears statistics about the packet processing rate of every module. FS# clear ip dhcp server rate	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.10 clear ip dhcp server statistics

	Use this command to reset the counter of the DHCP server in the privileged user mode.	
	clear ip dhcp server statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	The DHCP server carries out the statistics counter, records the DHCP address pool, automatic binding, manual binding and expired binding. Furthermore, it also carries out the statistics to the number of sent and received DHCP messages. The clear ip dhcp server statistics command can be used to delete the history counter record and carry out the statistics starting from scratch.	
Configuration Examples	The following example clears the statistics record of the DHCP server. <pre>clear ip dhcp server statistics</pre>	
Related Commands	Command	Description
	show ip dhcp server statistics	Displays the statistics record of the DHCP server.
Platform Description	N/A	

4.11 clear ip dhcp relay statistics

	Use this command to clear the DHCP relay statistics.	
	clear ip dhcp relay statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode	

Mode		
Usage Guide	The DHCP relay is configured with the counter to count various packets received or transmitted by the relay. This command is used to clear the counters.	
Configuration	The following example clears the DHCP relay statistics.	
Examples	FS# clear ip dhcp relay statistics	
Related		
Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

4.12 client-identifier

	Use this command to define the unique ID of the DHCP client (indicated in hex, separated by dot) in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	client-identifier <i>unique-identifier</i>	
	no client-identifier	
	default client-identifier	
Parameter Description	Parameter	Description
	<i>unique-identifier</i>	The DHCP client ID is indicated in hex and separated by dot, for instance, 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.
Defaults	N/A.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	When some DHCP clients request the DHCP server to assign IP addresses, they use their client IDs rather than their hardware addresses. The client ID consists of media type, MAC addresses and interface name. For instance, the MAC address is 00d0.f822.33b4, the interface name is GigabitEthernet 0/1, and the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where, 01 denotes the type of the Ethernet media. The 67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hex code of GigabitEthernet0/1. For the definition of the media code, refer to the Address Resolution Protocol Parameters section in RFC1700. This command is used only when the DHCP is defined by manual binding.	
Configuration Examples	The following example defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4. client-identifier 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31	

Related Commands	Command	Description
	hardware-address	Defines the hardware address of DHCP client.
	host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.13 client-name

	Use this command to define the name of the DHCP client in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	client-name <i>client-name</i>	
	no client-name	
	default client-name	
Parameter Description	Parameter	Description
	client-name	Name of DHCP client, a set of standards-based ASCII characters. The name should not include the suffix domain name. For instance, you can define the name of the DHCP client as river, not river.i-net.com.cn.
Defaults	No client name is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	This command can be used to define the name of the DHCP client only when the DHCP is defined by manual binding. This name should not include the suffix domain name.	
Configuration Examples	The following example defines a string river as the name of the client.	
	FS(dhcp-config)# client-name river	
Related Commands	Command	Description
	host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.14 default-router

	Use this command to define the default gateway of the DHCP client in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	default-router <i>ip-address</i> [<i>ip-address2...ip-address8</i>]	
	no default-router	
	default default-router	
Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the equipment. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 gateways can be configured.
Defaults	No gateway is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	In general, the DHCP client should get the information of the default gateway from the DHCP server. The DHCP server should specify one gateway address for the client at least, and this address should be of the same network segment as the address assigned to the client.	
Configuration Examples	The following example defines 192.168.12.1 as the default gateway. default-router 192.168.12.1	
Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.15 dns-server

	Use this command to define the DNS server of the DHCP client in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	dns-server { <i>ip-address</i> [<i>ip-address2...ip-address8</i>]	
	no dns-server	
	default dns-server	
Parameter	Parameter	Description
Description	<i>ip-address</i>	Defines the IP address of the DNS server. At least one IP address should be configured.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 DNS servers can be configured.

Defaults	No DNS server is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	When more than one DNS server is defined, the former will possess higher priority, so the DHCP client will select the next DNS server only when its communication with the former DNS server fails.	
Configuration	The following example specifies the DNS server 192.168.12.3 for the DHCP client.	
Examples	FS(dhcp-config)# dns-server 192.168.12.3	
Related Commands	Command	Description
	domain-name	Defines the suffix domain name of the DHCP client.
	ip address dhcp	Enables the DHCP client on the interface to obtain the IP address information.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.16 domain-name

	Use this command to define the suffix domain name of the DHCP client in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	domain-name <i>domain-name</i>	
	no domain-name	
	default domain-name	
Parameter Description	Parameter	Description
	domain-name	Defines the suffix domain name string of the DHCP client.
Defaults	No suffix domain name by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	After the DHCP client obtains specified suffix domain name, it can access a host with the same suffix domain name by the host name directly.	
Configuration Examples	The following example defines the suffix domain name i-net.com.cn for the DHCP client. FS(dhcp-config)#domain-name FS.com.cn	

Related Commands	Command	Description
	dns-server	Defines the DNS server of the DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
Platform Description	N/A	

4.17 force-no-router

	Use this command to cancel gateway allocation to the client. Use the no or default form of this command to restore the default setting.	
	force-no-router	
	no force-no-router	
	default force-no-router	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	DHCP address pool configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example cancels gateway allocation to the client. FS(dhcp-config)# force-no-router	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.18 hardware-address

	Use this command to cancel gateway allocation to the client. Use the no or default form of this command to restore the default setting.	
	force-no-router	
	no force-no-router	
	default force-no-router	
Parameter	Parameter	Description

Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	DHCP address pool configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example cancels gateway allocation to the client. FS(dhcp-config)# force-no-router	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.19 host

	Use this command to define the IP address and network mask of the DHCP client host in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	host <i>ip-address</i> [<i>netmask</i>]	
	no host	
	default host	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Defines the IP address of DHCP client.
	<i>netmask</i>	Defines the network mask of DHCP client.
Defaults	No IP address or network mask of the host is defined.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	If the network mask is not defined definitely, the DHCP server will use the natural network mask of this IP address: 255.0.0.0 for class A IP address, 255.255.0 for class B IP address, and 255.255.255.0 for class C IP address. This command can be used only when the DHCP is defined by manual binding.	
Configuration Examples	The following example sets the client IP address as 192.168.12.91, and the network mask as 255.255.255.240. host 192.168.12.91 255.255.255.240	
Related Commands	Command	Description
	client-identifier	Defines the unique ID of the DHCP client (Indicated in hex and separated

		by dot).
	hardware-address	Defines the hardware address of DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
default-router	Define the default route of the DHCP client.	default-router
Platform	N/A	
Description		

4.20 ip address dhcp

	Use this command to make the Ethernet interface or the PPP, HDLC and FR encapsulated interface obtain the IP address information by the DHCP in the interface configuration mode. Use the no or default form of this command to restore the default setting.	
	ip address dhcp	
	no ip address dhcp	
	default ip address dhcp	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The interface cannot obtain the IP address by the DHCP by default.	
Command Mode	Interface configuration mode.	
Usage Guide	When requesting the IP address, the DHCP client of the FSOS software also requires the DHCP server provide 5 configuration parameter information: 1) DHCP option 1, client subnet mask, 2) DHCP option 3, it is the same as the gateway information of the same subnet, 3) DHCP option 6, the DNS server information, 4) DHCP option 15, the host suffix domain name, and 5) DHCP option 44, the WINS server information (optional). The client of the FSOS software is allowed to obtain the address on the PPP, FR or HDL link by the DHCP, which should be supported by the server. At present, our server can support this function.	
Configuration Examples	The following example makes the FastEthernet 0 port obtain the IP address automatically. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1) ip address dhcp</pre>	
Related Commands	Command	Description
	dns-server	Defines the DNS server of DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform	N/A	

Description	

4.21 ip dhcp arp-probe

	Use this command to check ARP entries of the local host to prevent IP address conflict of an STA configured with a static IP address. Use the no form of this command to disable the function. Use the default form of this command to restore the default setting.	
	ip dhcp arp-probe	
	no ip dhcp arp-probe	
	default ip dhcp arp-probe	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The ARP entry check function is disabled by default.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This function is a supplement to the ping conflict detection function. If there is an STA with a static IP address and L2 isolation in the environment and the ping conflict detection function becomes invalid (for example, the firewall is enabled on the STA), an STA that applies for a dynamic address may be assigned with this IP address, resulting in IP conflict. This function can be enabled only in the preceding scenario. If ARP attack exists, this function cannot be enabled. Otherwise, the DHCP IP address assignment service is affected. As a result, it takes a long time for an STA to apply for an IP address or the STA cannot apply for an IP address.	
Configuration Examples	The following example enables the function in global configuration mode. <pre>FS(config)# ip dhcp arp-probe</pre>	
Verification	Run the show run command to check whether the configuration is successful.	

4.22 ip dhcp class

	Use this command to define a CLASS and enter the global CLASS configuration mode. Use the no form of this command to restore the default setting.	
	ip dhcp class class-name	
	no ip dhcp class class-name	
Parameter Description	Parameter	Description
	class-name	Class name, which can be character string or numeric such as myclass or 1.

Defaults	By default, the class is not configured.	
Command Mode	Global configuration mode.	
Usage Guide	After executing this command, it enters the global CLASS configuration mode which is shown as "FS (config-dhcp-class)#". In this configuration mode, user can configure the Option82 information that matches the CLASS and the CLASS identification information.	
Configuration Examples	The following example configures a global CLASS. FS(config)# ip dhcp class myclass	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.23 ip dhcp excluded-address

	Use this command to configure excluded IP address. Use the no or default form of this command to restore the default setting.	
	ip dhcp excluded-address <i>low-ip-address</i> [<i>high-ip-address</i>]	
	no ip dhcp excluded-address <i>low-ip-address</i> [<i>high-ip-address</i>]	
	default ip dhcp excluded-address <i>low-ip-address</i> [<i>high-ip-address</i>]	
Parameter Description	Parameter	Description
	<i>low-ip-address</i>	Indicates a start IP address.
	<i>high-ip-address</i>	Indicates an end IP address.
Defaults	By default, the DHCP server assigns all IP addresses of the address pool.	
Command Mode	Global configuration mode.	
Usage Guide	Unless otherwise specified, a DHCP server assigns all the addresses from an IP address pool to DHCP clients. To reserve some addresses(e.g., addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, it is recommended to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.	
Configuration Examples	The following example configures 192.168.12.100~150 as excluded IP address. FS(config)#ip dhcp excluded-address 192.168.12.100 192.168.12.150	

	The following example restores the default setting.	
	FS(config)#no ip dhcp excluded-address 192.168.12.100 192.168.12.150	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.24 ip dhcp force-send-nak

	Use this command to configure the forcible NAK packet sending function. Use the no or default form of this command to restore the default setting.	
	ip dhcp force-send-nak	
	no ip dhcp force-send-nak	
	default ip dhcp force-send-nak	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	The DHCP client checks the previously used IP address every time it is started and sends a DHCPREQUEST packet to continue leasing this IP address. If the address is not available, the DHCP server sends an NAK packet to let the client resend a DHCPDISCOVER packet to apply for a new IP address. If no corresponding lease record can be found on the server, the client keeps sending DHCPDISCOVER packets.	
Configuration Examples	The following example enables the forcible NAK packet sending function in global configuration mode. FS(config)# ip dhcp force-send-nak	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.25 ip dhcp ping packets

	Use this command to configure the times of ping the IP address when the DHCP server detects address conflict in the global configuration mode. Use the no or default form of this command to restore the default

	setting.	
	ip dhcp ping packets [<i>number</i>]	
	no ip dhcp ping packets	
	default ip dhcp ping packets	
Parameter	Parameter	Description
Description	<i>number</i>	(Optional) Number of packets in the range of 0 to 10, where 0 indicates disabling the ping operation. The Ping operation sends two packets by default.
Defaults	The Ping operation sends two packets by default.	
Command Mode	Global configuration mode.	
Usage Guide	When the DHCP server attempts to assign the IP address from the DHCP address pool, use the ping operation to check whether this address is occupied by other hosts. Record it if the address is occupied, otherwise, assign it to the DHCP client. The Ping operation will send up to 10 packets, two packets by default.	
Configuration Examples	The following example sets the number of the packets sent by the ping operation as 3.	
	FS(config)# ip dhcp ping packets 3	
Related Commands	Command	Description
	clear ip dhcp conflict	Clears the DHCP history conflict record.
	ip dhcp ping packet	Configures the timeout time that the DHCP server waits for the Ping response. If all the ping packets are not responded within the specified time, it indicates that this IP address can be assigned. Otherwise, it will record the address conflict.
	show ip dhcp conflict	Displays the DHCP server detects address conflict when it assigns an IP address.
Platform Description	N/A	

4.26 ip dhcp ping timeout

	Use this command to configure the timeout that the DHCP server waits for response when it uses the ping operation to detect the address conflict in the global configuration mode. Use the no or default form of this command to restore the default setting.	
	ip dhcp ping timeout <i>milli-seconds</i>	
	no ip dhcp ping timeout	
	default ip dhcp ping timeout	
Parameter	Parameter	Description
Description	<i>milli-seconds</i>	Time that the DHCP server waits for ping response in the range 100 to 10000 milliseconds.

Defaults	The default is 500 seconds.								
Command Mode	Global configuration mode.								
Usage Guide	This command defines the time that the DHCP server waits for a ping response packet.								
Configuration Examples	The following example configures the waiting time of the ping response packet to 600ms. <pre>ip dhcp ping timeout 600</pre>								
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>clear ip dhcp conflict</td><td>Clears the DHCP history conflict record.</td></tr> <tr> <td>ip dhcp ping packets</td><td>Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.</td></tr> <tr> <td>show ip dhcp conflict</td><td>Displays the address conflict the DHCP server detects when it assigns an IP address.</td></tr> </table>	Command	Description	clear ip dhcp conflict	Clears the DHCP history conflict record.	ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.	show ip dhcp conflict	Displays the address conflict the DHCP server detects when it assigns an IP address.
Command	Description								
clear ip dhcp conflict	Clears the DHCP history conflict record.								
ip dhcp ping packets	Defines the number of the data packets sent by the ping operation for the detection of the address conflict when the DHCP server assigns an IP address.								
show ip dhcp conflict	Displays the address conflict the DHCP server detects when it assigns an IP address.								
Platform Description	N/A								

4.27 ip dhcp pool

	Use this command to define a name of the DHCP address pool and enter the DHCP address pool configuration mode in the global configuration mode. Use the no or default form of this command to restore the default setting.				
	ip dhcp pool <i>pool-name</i>				
	no ip dhcp pool <i>pool-name</i>				
	default ip dhcp pool <i>pool-name</i>				
Parameter Description	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td><i>pool-name</i></td><td>A string of characters and positive integers, for instance, mypool or 1.</td></tr> </table>	Parameter	Description	<i>pool-name</i>	A string of characters and positive integers, for instance, mypool or 1.
Parameter	Description				
<i>pool-name</i>	A string of characters and positive integers, for instance, mypool or 1.				
Defaults	No DHCP address pool is defined by default.				
Command Mode	Global configuration mode.				
Usage Guide	Execute the command to enter the DHCP address pool configuration mode: <pre>FS(dhcp-config)#</pre> In this configuration mode, configure the IP address range, the DNS server and the default gateway.				
Configuration Examples	The following example defines a DHCP address pool named mypool0. <pre>FS(config)#ip dhcp pool mypool0</pre>				

Related Commands	Command	Description
	host	Defines the IP address and network mask, which is used to configure the DHCP manual binding.
	ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
	network (DHCP)	Defines the network number and network mask of the DHCP address pool.
Platform Description	N/A	

4.28 ip dhcp relay check server-id

	Use this command to enable the ip dhcp relay check server-id function. Use the no form of this command to restore the default setting.	
	ip dhcp relay check server-id	
	no ip dhcp relay check server-id	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The ip dhcp relay check server-id command is disabled.	
Command Mode	Global configuration mode.	
Usage Guide	Switch will select the server to be sent according to server-id option when forwarding DHCP REQUEST via this command. Without this command configured, the switch forwards the DHCP REQUEST to all configured DHCP servers.	
Configuration Examples	The following example enables the ip dhcp relay check server-id function. <pre>FS(config)# ip dhcp relay check server-id</pre> The following example disables the ip-dhcp relay check server-id function. <pre>FS(config)# no ip dhcp relay check server-id</pre>	
Related Commands	Command	Description
	service dhcp	Enables the DHCP Relay.
Platform Description	N/A	

4.29 ip dhcp relay information option82

	Use this command to enable the ip dhcp relay information option82 function. Use the no form of this command to restore the default setting.	
	ip dhcp relay information option82	
	no ip dhcp relay information option82	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The ip dhcp relay information option82 command is disabled.	
Command Mode	Global configuration mode.	
Usage Guide	This command is exclusive with the option dot1x command.	
Configuration Examples	The following example enables the option82 function on the DHCP relay. <pre>FS(config)# ip dhcp relay information option82</pre> The following example disables the option82 function on the DHCP relay. <pre>FS(config)# no ip dhcp relay information option82</pre>	
Related Commands	Command	Description
	service dhcp	Enables the DHCP Relay.
Platform Description	N/A	

4.30 ip dhcp relay suppression

	Use this command to enable the DHCP binding globally. Use the no form of this command to disable the DHCP binding globally and enable the DHCP relay suppression on the port.	
	ip dhcp relay suppression	
	no ip dhcp relay suppression	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The ip dhcp relay suppression command is disabled.	
Command Mode	Interface configuration mode.	

Usage Guide	After executing this command, the system will not relay the DHCP request message on the interface.	
Configuration Examples	The following example enables the relay suppression function. FS(config-if)# ip dhcp relay suppression	
	The following example enables the relay suppression function. FS(config-if)# no ip dhcp relay suppression	
Related Commands	Command	Description
	service dhcp	Enables the DHCP Relay.
Platform Description	N/A	

4.31 ip dhcp server arp-detect

	Use this command to enable the user-offline detection. Use the no or default form this command to restore the default setting.	
	ip dhcp server arp-detect	
	no ip dhcp server arp-detect	
	default ip dhcp server arp-detect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to detect whether the user has gone offline, If the user does not go online within a certain period, the IP address is reclaimed.	
Configuration Examples	The following example enables the user-offline detection. FS(config)# ip dhcp server arp-detect	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.32 ip dhcp server detect

	Use this command to enable the fake DHCP server detection. Use the no or default form of this command to restore the default setting.	
	ip dhcp server detect	
	no ip dhcp server detect	
	default ip dhcp server detect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After this function is enabled, any fake DHCP server detected is logged.	
Configuration Examples	The following example enables the fake DHCP server detection.	
	FS(config)# ip dhcp server detect	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.33 ip dhcp use class

	Use this command to enable the CLASS to allocate addresses in the global configuration mode. Use the no form of this command can be used to disable the CLASS.	
	ip dhcp use class	
	no ip dhcp use class	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	Enabled	
Command Mode	This function is enabled by default.	
Usage Guide	N/A	
Configuration Examples	The following example enables the CLASS to allocate addresses.	
	FS(config)# ip dhcp use class	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.34 ip helper-address

	Use this command to add an IP address of the DHCP server. Use the no form of this command to delete an IP address of the DHCP server. The server address can be configured globally or on a specific interface. Therefore, this command can run in the global configuration mode or the interface configuration mode to add the DHCP server information.	
	ip helper-address { cycle-mode [vrf {vrf-name}] A.B.C.D }	
	no ip helper-address { cycle-mode [vrf {vrf-name}] A.B.C.D }	
Parameter Description	Parameter	Description
	cycle-mode	Indicates that DHCP request packets are forwarded to all DHCP servers.
	vrf {vrf-name}	Indicates a VPN Routing & Forwarding (VRF) name.
	A.B.C.D	Indicates the IP address of a DHCP server.
Defaults	N/A	
Command Mode	Global configuration mode, interface configuration mode.	
Usage Guide	DHCP request packets are sent to the DHCP server whose IP address is configured, while DHCP response packets are forwarded to the DHCP client. Up to 20 DHCP server IP addresses can be configured globally or on a layer-3 interface. When an interface receives a DHCP request packet, the DHCP server configuration on the interface prevails over that configured globally. If the interface is not configured with DHCP server addresses, the global configuration takes effect. DHCP relay is based on vrf. In global configuration mode, you can enable cycle-mode. When it is enabled, DHCP request packets are forwarded to all DHCP servers. If it is not enabled, DHCP request packets are sent to the first DHCP server configured under this rule. This parameter can only be enabled in global configuration mode and take effect both globally and on interfaces. By default, cycle-mode is enabled.	
Configuration Examples	The following example sets the address for a DHCP server, in the interface vlan 1, to 192.168.11.1. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# interface vlan 1 FS(config-if)# ip helper-address 192.168.11.1</pre> The following example deletes the configured address of a DHCP server, 192.168.11.1.	

	<pre>FS(config-if)# no ip helper-address 192.168.11.1</pre> The following example sets the IP address for the global server to 192.168.100.1. <pre>FS# configure terminal</pre> Enter configuration commands, one per line. End with CNTL/Z. <pre>FS(config)# ip helper-address 192.168.100.1</pre> The following example deleted the configured IP address for the global server, 192.168.100.1. <pre>FS(config)# no ip helper-address 192.168.100.1</pre> The following example enables DHCP request packets to be forwarded to all servers. <pre>FS(config)# ip helper-address cycle-mode</pre> The following example disables DHCP request packets to be forwarded to all servers. <pre>FS(config)# no ip helper-address cycle-mode</pre>	
Related Commands	Command	Description
	service dhcp	Enables the DHCP relay.
Platform Description	N/A	

4.35 lease

	Use this command to define the lease time of the IP address that the DHCP server assigns to the client in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting. A limited lease time ranges from 1 minute to 23 hours and 59 minutes.	
	lease { days [hours] [minutes] infinite }	
	no lease	
	default lease	
Parameter Description	Parameter	Description
	days	Lease time in days
	hours	(Optional) Lease time in hours. It is necessary to define the days before defining the hours.
	minutes	(Optional) Lease time in minutes. It is necessary to define the days and hours before defining the minutes.
	infinite	Infinite lease time.
Defaults	The lease time for a static address pool is infinite. The lease time for other address pools is 1 day.	
Command Mode	DHCP address pool configuration mode.	

Usage Guide	When the lease is getting near to expire, the DHCP client will send the request of renewal of lease. In general, the DHCP server will allow the renewal of lease of the original IP address.					
Configuration Examples	The following example sets the DHCP lease to 1 hour. <pre>FS(dhcp-config)# lease 0 1</pre> The following example sets the DHCP lease to 1 minute. <pre>FS(dhcp-config)# lease 0 0 1</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp pool</td><td>Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.</td></tr></table>	Command	Description	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.	
Command	Description					
ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.					
Platform Description	N/A					

4.36 lease-threshold

	Use this command in DHCP address pool configuration mode to define the DHCP alarm threshold. Use the default or no form of this command to restore the default setting.	
	lease-threshold <i>percentage</i>	
	default lease-threshold	
	no lease-threshold	
Parameter Description	Parameter	Description
	<i>percentage</i>	Usage of the address pool, ranging from 60 to 100 in percentage.
Defaults	90	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	If the maximum IP usage of the address pool reaches the threshold, the DHCP Server generates a SYSLOG alarm. The IP usage indicates the ratio of the number of assigned address pools to the total number of assignable address pools. If the number of assigned pools stays above the alarm threshold, an alarm is generated every 5 minutes.	
Configuration Examples	The following example sets the alarm threshold to 80%. FS(dhcp-config)# lease-threshold 80 The following example disables the address pool alarm function. FS(dhcp-config)# no lease-threshold	

Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.37 match ip

	Use this command to define an AM matching rule. Use the no form of this command to remove the configuration. Use the clear form of this command to clear all configurations.	
	match ip ip-address netmask [interface] [add/remove] vlan vlan-list	
	no match ip ip-address netmask [interface] [add/remove] vlan vlan-list	
	clear match ip [interface]	
Parameter Description	Parameter	Description
	ip-address	IP address
	netmask	Subnet mask
	interface	Interface ID
	add/remove	Adds or removes the specified VLAN.
	vlan-list	VLAN ID
Defaults	N/A	
Command Mode	AM rule configuration mode	
Usage Guide	With this function enabled, all DHCP clients with specified vlan-list and interface obtain addresses in the rule. If a DHCP client obtains a static address, it is not subject to AM matching rules in whichever Sub VLAN unless the AM rule configuration is based on VLAN instead of Sub VLAN. This type of matching rules applies to only static addresses.	
Configuration Examples	The following example defines an AM matching rule. <pre>FS(config-address-manage)#match ip 192.168.11.0 255.255.255.0 GigabitEthernet 0/10 vlan 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.38 match ip default

	Use this command to define a default AM matching rule. Use the no form of this command to remove the configuration,	
	match ip default ip-address netmask	
	no match ip default ip-address netmask	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address
	<i>netmask</i>	Subnet mask
Defaults	N/A	
Command Mode	AM rule configuration mode	
Usage Guide	With this function enabled, all DHCP clients with specified vlan-list and interface obtain addresses in the default rule.	
Configuration Examples	The following example defines a default AM matching rule. FS(config-address-manage)#match ip default 192.168.12.0 255.255.255.0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.39 netbios-name-server

	Use this command to configure the WINS name server of the Microsoft DHCP client NETBIOS in the DHCP address pool configuration mode. The no or default form of this command can be used to restore the default setting.	
	netbios-name-server ip-address [ip-address2...ip-address8]	
	no netbios-name-server	
	default netbios-name-server	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address of the WINS server. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) IP addresses of WINS servers. Up to 8 WINS servers can be configured.
Defaults	No WINS server is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	When more than one WINS server is defined, the former has higher priority. The DHCP client will select the next	

	WINS server only when its communication with the former WINS server fails.	
Configuration Examples	The following example specifies the WINS server 192.168.12.3 for the DHCP client.	
	netbios-name-server 192.168.12.3	
Related Commands	Command	Description
	ip address dhcp	Enables the DHCP client on the interface to obtain the IP address.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	netbios-node-type	Defines the netbios node type of the client host.
Platform Description	N/A	

4.40 netbios-node-type

	Use this command to define the node type of the master NetBIOS of the Microsoft DHCP client in the DHCP address configuration mode. Use the no or default form of this command to restore the default setting.	
	netbios-node-type type	
	no netbios-node-type	
	default netbios-node-type	
Parameter Description	Parameter	Description
	type	Type of node in two modes: Digit in hexadecimal form in the range of 0 to FF. Only the following numerals are available: 1: b-node. 2: p-node. 4: m-node. 8: h-node. String: b-node: broadcast node p-node: peer-to-peer node m-node: mixed node h-node: hybrid node
Defaults	No type of the NetBIOS node is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	There are 4 types of the NetBIOS nodes of the Microsoft DHCP client: 1) Broadcast, which carries out the NetBIOS name resolution by the broadcast method, 2) Peer-to-peer, which directly requests the WINS server to carry out the NetBIOS name resolution, 3) Mixed, which requests the name resolution by the broadcast method firstly, and	

	then carry out the name resolution by the WINS server connection, 4) Hybrid, which requests the WINS server to carry out the NetBIOS name resolution firstly, and it will carry out the NetBIOS name resolution by the broadcast method if the response is not received. By default, the node type for Microsoft operating system is broadcast or hybrid. If the WINS server is not configured, broadcast node is used. Otherwise, hybrid node is used. It is recommended to set the type of the NetBIOS node as Hybrid.							
Configuration Examples	The following example sets the NetBIOS node of Microsoft DHCP client as Hybrid. <pre>FS(dhcp-config)# netbios-node-type h-node</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp pool</td><td>Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.</td></tr><tr><td>netbios-name-server</td><td>Configures the WINS name server of the Microsoft DHCP client NETBIOS.</td></tr></table>	Command	Description	ip dhcp pool	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.	netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.	
Command	Description							
ip dhcp pool	Defines the name of DHCP address pool and enters the DHCP address pool configuration mode.							
netbios-name-server	Configures the WINS name server of the Microsoft DHCP client NETBIOS.							
Platform Description	N/A							

4.41 network

	Use this command to define the network number and network mask of the DHCP address pool in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	network <i>net-number net-mask</i> [<i>low-ip-address high-ip-address</i>]	
	no network	
	default network	
Parameter Description	Parameter	Description
	<i>net-number</i>	Network number of the DHCP address pool
	<i>net-mask</i>	Network mask of the DHCP address pool. If the network mask is not defined, the natural network mask will be used by default.
	<i>low-ip-address</i>	Start IP address.
	<i>high-ip-address</i>	End IP address.
Defaults	No network number or network mask is defined by default.	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	This command defines the subnet and subnet mask of a DHCP address pool, and provides the DHCP server with an address space which can be assigned to the clients. Unless excluded addresses are configured, all the addresses of the DHCP address pool can be assigned to the clients. The DHCP server assigns the addresses in the address pool orderly. If the DHCP server found an IP address is in the DHCP binding table or in the network segment, it checks the next until it assigns an effective IP address. The show ip dhcp binding command can be used to view the address assignment, and the show ip dhcp	

	conflict command can be used to view the address conflict detection configuration.	
Configuration Examples	The following example defines the network number of the DHCP address pool as 192.168.12.0, and the network mask as 255.255.255.240. <pre>network 192.168.12.0 255.255.255.240</pre>	
Related Commands	Command	Description
	ip dhcp excluded-address	Defines the IP addresses that the DHCP server cannot assign to the clients.
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.
Platform Description	N/A	

4.42 next-server

	Use this command to define the startup sever list that the DHCP client accesses during startup in the DHCP address configuration mode. Use the no or default form of this command to restore the default setting.	
	next-server <i>ip-address</i> [<i>ip-address2...ip-address8</i>]	
	no next-server	
	default next-server	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Defines the IP address of the startup server, which is usually the TFTP server. It is required to configure one IP address at least.
	<i>ip-address2...ip-address8</i>	(Optional) Up to 8 startup servers can be configured.
Defaults	N/A	
Command Mode	DHCP address pool configuration mode.	
Usage Guide	When more than one startup server is defined, the former will possess higher priory. The DHCP client will select the next startup server only when its communication with the former startup server fails.	
Configuration Examples	The following example specifies the startup server 192.168.12.4 for the DHCP client. <pre>FS(dhcp-config)# next-server 192.168.12.4</pre>	
Related Commands	Command	Description
	bootfile	Defines the default startup mapping file name of the DHCP client.
	ip dhcp pool	Defines the name of the DHCP address pool and enter the DHCP address pool configuration mode.
	ip help-address	Defines the Helper address on the interface.
	option	Configures the option of the FSOS software DHCP server.

Platform	N/A
Description	

4.43 option

	Use this command to configure the option of the DHCP server in the DHCP address pool configuration mode. Use the no or default form of this command to restore the default setting.	
	option <i>code</i> { ascii <i>string</i> hex <i>string</i> ip <i>ip-address</i> }	
	no option	
	default option	
Parameter Description	Parameter	Description
	code	Defines the DHCP option codes.
	ascii string	Defines an ASCII string.
	hex string	Defines a hex string.
	ip ip-address	Defines an IP address list.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	The DHCP provides a mechanism to transmit the configuration information to the host in the TCP/IP network. The DHCP message has a variable option field that can be defined according to the actual requirement. The DHCP client needs to carry the DHCP message with 32 bytes of option information at least. Furthermore, the fixed data field in the DHCP message is also referred to as an option. For the definition of current DHCP option, refer to RFC 2131.	
Configuration Examples	The following example defines the option code 19, which determines whether the DHCP client can enable the IP packet forwarding. 0 indicates to disable the IP packet forwarding, and 1 indicates to enable the IP packet forwarding. The configuration below enable the IP packet forwarding on the DHCP client. <pre>FS(dhcp-config)# option 19 hex 1</pre> The following example defines the option code 33, which provides the DHCP client with the static route information. The DHCP client will install two static routes: 1) the destination network 172.16.12.0 and the gateway 192.168.12.12, 2) the destination network 172.16.16.0 and the gateway 192.168.12.16. <pre>option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16</pre>	
Related Commands	Command	Description
	ip dhcp pool	Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.

Platform	N/A
Description	

4.44 pool-status

	Use this command to enable or disable the DHCP address pool.	
	pool-status { enable disable }	
Parameter	Parameter	Description
Description	enable	Enables the address pool.
	disable	Disables the address pool.
Defaults	By default, the address pool is enabled after it is configured.	
Command Mode	DHCP address pool configuration mode	
Usage Guide	This command is configured on the DHCP server.	
Configuration Examples	The following example disables the address pool.	
	FS(dhcp-config)# pool-status disable	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

4.45 relay agent information

	Use this command to enter the Option82 matching information configuration mode in the global CLASS configuration mode. Use the no form of this command to delete the Option82 matching information of the CLASS.	
	relay agent information	
	no relay agent information	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Global CLASS configuration mode	

Usage Guide	After executing this command, it enters the Option82 matching information configuration mode which is shown as "FS (config-dhcp-class-relayinfo)#". In this configuration mode, user can configure the class matching multiple Option82 information.	
Configuration Examples	The following example configures a global CLASS and enters the Option82 matching information configuration mode. FS(config)# ip dhcp class myclass FS(config-dhcp-class)# relay agent information FS(config-dhcp-class-relayinfo)#	
Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enters the global CLASS configuration mode.
Platform Description	N/A	

4.46 relay-information hex

	Use this command to enter the Option82 matching information configuration mode. Use the no form of this command to delete a piece of matching information.					
	relay-information hex <i>aabb.ccdd.eeff... [*]</i>					
	no relay-information hex <i>aabb.ccdd.eeff... [*]</i>					
Parameter Description	<table><tr><th>Parameter</th><th>Description</th></tr><tr><td><i>aabb.ccdd.eeff...[*]</i></td><td>Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.</td></tr></table>	Parameter	Description	<i>aabb.ccdd.eeff...[*]</i>	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.	
Parameter	Description					
<i>aabb.ccdd.eeff...[*]</i>	Hexadecimal Option82 matching information. The '*' symbol means partial matching which needs the front part matching only. Without the '*' means needing full matching.					
Defaults	N/A					
Command Mode	Global CLASS configuration mode					
Usage Guide	N/A					
Configuration Examples	The following example configures a global CLASS which can match multiple Option82 information. <pre>FS(config)# ip dhcp class myclass FS(config-dhcp-class)# relay agent information FS(config-dhcp-class-relayinfo)# relay-information hex 0102256535 FS(config-dhcp-class-relayinfo)# relay-information hex 010225654565 FS(config-dhcp-class-relayinfo)# relay-information hex 060225654565</pre>					

	FS(config-dhcp-class-relayinfo)# relay-information hex 060223*	
Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.
	relay agent information	Enters the Option82 matching information configuration mode.
Platform Description	N/A	

4.47 remark

	Use this command to configure the identification which is used to describe the CLASS in this global CLASS configuration mode. Use the no form of this command to delete the identification.	
	remark <i>class-remark</i>	
	no remark	
Parameter Description	Parameter	Description
	class-remark	Information used to identify the CLASS, which can be the character strings with space in them.
Defaults	N/A.	
Command Mode	Global CLASS configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the identification information for a global CLASS. FS(config)# ip dhcp class myclass FS(config-dhcp-class)# remark used in #1 build	
Related Commands	Command	Description
	ip dhcp class	Defines a CLASS and enter the global CLASS configuration mode.
Platform Description	N/A	

4.48 service dhcp

	Use this command to enable the DHCP server and the DHCP relay on the device in global configuration mode. Use the no or default form of this command to restore the default setting.	
	service dhcp	
	no service dhcp	

	default service dhcp	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The service dhcp command is disabled.	
Command Mode	Global configuration mode	
Usage Guide	The DHCP server can assign the IP addresses to the clients automatically, and provide them with the network configuration information such as DNS server and default gateway. The DHCP relay can forward the DHCP requests to other servers, and the returned DHCP responses to the DHCP client, serving as the relay for DHCP packets.	
Configuration Examples	The following example enables the DHCP server and the DHCP relay feature. FS(config)# service dhcp	
Related Commands	Command	Description
	show ip dhcp server statistics	Displays various statistics information of the DHCP server.
	ip helper-address [vrf] A.B.C.D	Adds an IP address of the DHCP server.
Platform Description	N/A	

4.49 show dhcp lease

	Use this command to display the lease information of the IP address obtained by the DHCP client.	
	show dhcp lease	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	If the IP address is not defined, display the binding condition of all addresses. If the IP address is defined, display the binding condition of this IP address.	
Configuration Examples	The following example displays the result of the show dhcp lease. FS# show dhcp lease Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0	

	Temp sub net mask: 255.255.255.0 DHCP Lease server: 192.168.5.70, state: 3 Bound DHCP transaction id: 168F Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs Temp default-gateway addr: 192.168.5.1 Next timer fires after: 00:04:29 Retry count: 0 Client-ID: redgaint-00d0.f8fb.5740-Fa0/0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.50 show ip dhcp binding

	Use this command to display the binding condition of the DHCP address.		
	show ip dhcp binding [<i>ip-address</i>]		
Parameter	Parameter	Description	
Description	<i>ip-address</i>	(Optional) Only displays the binding condition of the specified IP addresses.	
Defaults	N/A		
Command Mode	Privileged EXEC mode.		
Usage Guide	If the IP address is not defined, show the binding condition of all addresses. If the IP address is defined, show the binding condition of this IP address		
Configuration Examples	The following is the result of the show ip dhcp binding. <pre>FS# show ip dhcp binding Total number of clients : 4 Expired clients : 3 Running clients : 1 IP address Hardware address Lease expiration Type 20.1.1.1 2000.0000.2011 000 days 23 hours 59 mins Automatic</pre> The meaning of various fields in the show result is described as follows.		

	Field	Description
	IP address	The IP address to be assigned to the DHCP client.
	Client-Identifier /Hardware address	The client identifier or hardware address of the DHCP client.
	Lease expiration	The expiration date of the lease. The Infinite indicates it is not limited by the time. The IDLE indicates the address is in the free status currently for it is not renewed or the DHCP client releases it actively.
	Type	The type of the address binding. The Automatic indicates an IP address is assigned automatically, and the Manual indicates an IP address is assigned by manual.
Related Commands	Command	Description
	clear ip dhcp binding	Clears the DHCP address binding table.
Platform Description	N/A	

4.51 show ip dhcp conflict

	Use this command to show the conflict history record of the DHCP sever.	
	show ip dhcp conflict	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command can display the conflict address list detected by the DHCP server.	
Configuration Examples	The following example displays the output result of the show ip dhcp conflict command.	
	FS# show ip dhcp conflict	
	IP address Detection Method	
	192.168.12.1 Ping	
	The meaning of various fields in the show result is described as follows.	
	Field	Description
	IP address	The IP addresses which cannot be assigned to the DHCP client.
	Detection Method	The conflict detection method.

Related Commands	Command	Description
	clear ip dhcp conflict	Clears the DHCP conflict record.
Platform Description	N/A	

4.52 show ip dhcp database

	Use this command to display backup status of DHCP database.															
	show ip dhcp database															
Parameter	Parameter	Description														
Description	N/A	N/A														
Defaults	N/A															
Command Mode	Privileged EXEC mode.															
Usage Guide	This command is configured on the DHCP server. Run this command to display information about the DHCP database.															
Configuration Examples	The following example displays status of the DHCP database.. <pre>FS#show ip dhcp database Enable :No Status :ready Save File :Default Successss :0 Failures :0 Interval Time :86400</pre> The meaning of various fields in the show result is described as follows. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Enable</td><td>The status of the database.</td></tr><tr><td>Status</td><td>The status of data recovery.</td></tr><tr><td>Save File</td><td>The path where data is saved.</td></tr><tr><td>Successss</td><td>The times of successful data saving.</td></tr><tr><td>Failures</td><td>The times of failed data saving.</td></tr><tr><td>Interval Time</td><td>The interval time for data saving.</td></tr></table>		Field	Description	Enable	The status of the database.	Status	The status of data recovery.	Save File	The path where data is saved.	Successss	The times of successful data saving.	Failures	The times of failed data saving.	Interval Time	The interval time for data saving.
Field	Description															
Enable	The status of the database.															
Status	The status of data recovery.															
Save File	The path where data is saved.															
Successss	The times of successful data saving.															
Failures	The times of failed data saving.															
Interval Time	The interval time for data saving.															

Related Commands	N/A
Platform Description	N/A

4.53 show ip dhcp history

	Use this command to display the DHCP lease history.	
	show ip dhcp history	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is configured on the DHCP server.	
Configuration Examples	The following example displays the DHCP lease history. <pre>FS#show ip dhcp history Expired clients : 3 IP address Hardware address Lease expiration Vlan/Relay 10.1.1.5 2222.abcd.47ac IDLE 4097 10.1.1.4 2222.abcd.47ae IDLE 4097 10.1.1.3 2222.abcd.47ad IDLE 4097 Running clients : 0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.54 show ip dhcp identifier

	Use this command to display the DHCP address pool ID and address usage.	
	show ip dhcp identifier	
Parameter	Parameter	Description
Description	N/A	N/A

Defaults	N/A					
Command Mode	Privileged EXEC mode					
Usage Guide	N/A					
Configuration Examples	The following example displays the DHCP address pool ID and address usage.					
	FS# show ip dhcp identifier					
	Pool	name	Identifier	Total	Distributed	Remained
	-----	-----	-----	-----		
	wwp		597455782	65533	0	65533
	Pool name			Address pool name.		
	Identifier			Address pool ID.		
	Total			Total number of addresses.		
	Distributed			Number of allocated addresses.		
	Remained			Number of remained addresses.		
Related Commands	Command			Description		
	N/A			N/A		
Platform Description	N/A					

4.55 show ip dhcp pool

	Use this command to display the address statistics of an address pool.	
	show ip dhcp pool [<i>poolname</i>]	
Parameter Description	Parameter	Description
	<i>poolname</i>	(Optional) Address pool whose address statistics are to be displayed.
Defaults	Privileged EXEC mode.	
Command Mode	N/A	
Usage Guide	Use this command to show the address statistics of an address pool.	
Configuration Examples	The following example displays the output result of the show ip dhcp pool <i>poolname</i> command.	
	FS# show ip dhcp pool	

	FS#sh ip dh pool					
	Pool	name	Total	Distributed	Remained	Percentage
	-----	-----	-----	-----	-----	
	net20		253	11	242	4.34782
	test		0	0	0	0.00000
Related Commands	Command		Description			
	ip dhcp pool		Defines the name of the DHCP address pool and enters the DHCP address pool configuration mode.			
Platform Description	N/A					

4.56 show ip dhcp relay-statistics

	Use this command to display the statistics of the DHCP relay.	
	show ip dhcp relay-statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the statistics of the DHCP relay.	
Configuration Examples	The following example displays the statistics of the DHCP relay.	
	<pre> FS# show ip dhcp relay-statistics Cycle mode 0 Message Count Discover 0 Offer 0 Request 0 Ack 0 Nak 0 Decline 0 Release 0 Info 0 Bad 0 Direction Count </pre>	

	Rx client 0 Rx client uni 0 Rx client bro 0 Tx client 0 Tx client uni 0 Tx client bro 0 Rx server 0 Tx server 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.57 show ip dhcp server detect

	Use this command to display the fake DHCP server detected.	
	show ip dhcp server detect	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the fake DHCP server detected.	
	FS#show ip dhcp server detect The DHCP Server information: Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.58 show ip dhcp server statistics

	Use this command to display the statistics of the DHCP server.	
	show ip dhcp server statistics	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command displays the statistics of the DHCP server.	
Configuration Examples	The following example displays the output result of the show ip dhcp server statistics command. <pre> FS# show ip dhcp server statistics Address pools 2 Lease counter 4 Active Lease Counter 0 Expired Lease Counter 4 Malformed messages 0 Dropped messages 0 Message Received BOOTREQUEST 216 DHCPDISCOVER 33 DHCPREQUEST 25 DHCPDECLINE 0 DHCPRELEASE 1 DHCPINFORM 150 Message Sent BOOTREPLY 16 DHCPOFFER 9 DHCPACK 7 DHCPNAK 0 DHCPREQTIMES 0 DHCPREQSUCTIMES 0 DISCOVER-PROCESS-ERROR 0 LEASE-IN-PINGSTATE 0 NO-LEASE-RESOURCE 0 SERVERID-NO-MATCH 0 </pre>	

<pre> ----- recv 0 send 0 </pre>															
The meaning of various fields in the show result is described as follows.															
<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Address pools</td><td>Number of address pools.</td></tr> <tr> <td>Automatic bindings</td><td>Number of automatic address bindings.</td></tr> <tr> <td>Manual bindings</td><td>Number of manual address bindings.</td></tr> <tr> <td>Expired bindings</td><td>Number of expired address bindings.</td></tr> <tr> <td>Malformed messages</td><td>Number of malformed messages received by the DHCP.</td></tr> <tr> <td>Message Received or Sent</td><td>Number of the messages received and sent by the DHCP server respectively.</td></tr> </table>		Field	Description	Address pools	Number of address pools.	Automatic bindings	Number of automatic address bindings.	Manual bindings	Number of manual address bindings.	Expired bindings	Number of expired address bindings.	Malformed messages	Number of malformed messages received by the DHCP.	Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.
Field	Description														
Address pools	Number of address pools.														
Automatic bindings	Number of automatic address bindings.														
Manual bindings	Number of manual address bindings.														
Expired bindings	Number of expired address bindings.														
Malformed messages	Number of malformed messages received by the DHCP.														
Message Received or Sent	Number of the messages received and sent by the DHCP server respectively.														
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>clear ip dhcp server statistics</td><td>Clears the DHCP server statistics.</td></tr> </table>	Command	Description	clear ip dhcp server statistics	Clears the DHCP server statistics.										
Command	Description														
clear ip dhcp server statistics	Clears the DHCP server statistics.														
Platform Description	N/A														

4.59 show ip dhcp socket

Use this command to display the socket used by the DHCP server.					
show ip dhcp socket					
Parameter Description	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Parameter	Description	N/A	N/A
Parameter	Description				
N/A	N/A				
Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	N/A				
Configuration Examples	The following example displays the socket used by the DHCP server. <pre> FS#show ip dhcp socket dhcp socket = 47. </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

5 DHCPv6 Commands

5.1 clear ipv6 dhcp binding

	Use this command to clear the DHCPv6 binding information.	
	clear ipv6 dhcp binding [<i>ipv6-address</i>]	
Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the IPv6 address or the prefix.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If the <i>ipv6-address</i> is not specified, all DHCPv6 binding information is cleared. If the <i>ipv6-address</i> is specified, the binding information for the specified address is cleared.	
Configuration Examples	The following example clears the DHCPv6 binding information: <pre>FS(config)# clear ipv6 dhcp binding</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.2 clear ipv6 dhcp client

	Use this command to reset the DHCPv6 client.	
	clear ipv6 dhcp client <i>interface-type interface-number</i>	
Parameter	Parameter	Description
Description	<i>interface-type interface-number</i>	Sets the interface type and the interface number.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to reset the DHCPv6 client, which may lead the client to request for the configurations from the server again.	

Configuration Examples	The following example resets DHCP client VLAN 1. FS# clear ipv6 dhcp client vlan 1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.3 clear ipv6 dhcp conflict

	Use this command to clear the DHCPv6 address conflicts.	
	clear ipv6 dhcp conflict { <i>ipv6-address</i> * }	
Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Specifies IPv6 address or prefix.
	*	All IPv6 addresses or prefixes
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If an IPv6 address conflict is detected, the DHCPv6 client will send the Decline message. Then the DHCPv6 server will add the address in this message into the address conflict queue. The addresses added into the address conflict queue cannot be assigned any longer. If the * parameter is not specified, all conflicts of IPv6 addresses or prefixes will be deleted. If the <i>ipv6-address</i> parameter is specified, only the specified address conflict will be deleted.	
Configuration Examples	The following example clears a DHCPv6 address conflict. FS# clear ipv6 dhcp conflict 2008:50::2	
Related Commands	Command	Description
	show ipv6 dhcp conflict	Displays address conflicts.
Platform Description	N/A	

5.4 clear ipv6 dhcp relay statistics

	Use this command to clear the packet sending and receiving condition with the DHCPv6 Relay function enabled.
	clear ipv6 dhcp relay statistics

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears the packet sending and receiving condition with the DHCPv6 Relay function enabled. FS# clear ipv6 dhcp relay statistics	
Related Commands	Command	Description
	show ipv6 dhcp relay statistics	Displays the statistical information.
Platform Description	N/A	

5.5 clear ipv6 dhcp server statistics

	Use this command to clear the DHCPv6 server statistics.	
	clear ipv6 dhcp server statistics	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the DHCPv6 server statistics.	
Configuration Examples	The following example clears the DHCPv6 server statistics.	
	FS(config)# clear ipv6 dhcp server statistics	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.6 dns-server

	Use this command to set the DNS Server list information for the DHCPv6 Server. Use the no form of this command to restore the default setting.	
	dns-server <i>ipv6-address</i>	
	no dns-server <i>ipv6-address</i>	
Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the IPv6 address or the DNS server.
Defaults	By default, no DNS server list is configured.	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	To configure several DNS Server addresses, use the dns-server command for several times. The newly-configured DNS Server address will not overwrite the former ones.	
Configuration Examples	The following example configures the DNS server address. FS(config-dhcp)# dns-server 2008:1::1	
Related Commands	Command	Description
	domain-name	Sets the DHCPv6 domain name information.
	ipv6 dhcp pool	Sets a DHCPv6 pool.
Platform Description	N/A	

5.7 domain-name

	Use this command to set the domain name for the DHCPv6 server. Use the no form of this command to restore the default setting.	
	domain-name <i>domain</i>	
	no domain-name <i>domain</i>	
Parameter	Parameter	Description
Description	<i>domain</i>	Sets the domain name.
Defaults	By default, no domain name is configured.	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	To configure several domain names, use the domain-name command for several times. The newly-configured	

	domain name will not overwrite the former ones.	
Configuration	The following example sets the domain name for the DHCPv6 server to example.com.	
Examples	FS(config-dhcp)# domain-name example.com	
Related Commands	Command	Description
	dns-server	Sets the DHCPv6 DNS server list.
	ipv6 dhcp pool	Sets the DHCPv6 pool.
Platform	N/A	
Description		

5.8 iana-address prefix

	Use this command to set the IA_NA address prefix for the DHCPv6 Server. Use the no form of this command to restore the default setting.	
	iana-address prefix <i>ipv6-prefix/prefix-length</i> [lifetime { <i>valid-lifetime</i> <i>preferred-lifetime</i> }]	
	no iana-address prefix	
Parameter Description	Parameter	Description
	<i>ipv6-prefix/prefix-length</i>	Sets the IPv6 prefix and prefix length.
	lifetime	Sets the lifetime of the address allocated to the client. With the keyword lifetime configured, both parameters <i>valid-lifetime</i> and <i>preferred-lifetime</i> shall be configured.
	<i>valid-lifetime</i>	Sets the valid lifetime of using the allocated address for the client.
	<i>preferred-lifetime</i>	Sets the preferred lifetime of the address allocated to the client.
Defaults	By default, no IA_NA address prefix is configured. The default <i>valid-lifetime</i> is 3,600s(1 hour). The default <i>preferred-lifetime</i> is 3,600s(1 hour).	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	This command is used to set the IA_NA address prefix for the DHCPv6 Server, and allocate the IA_NA address to the client. The Server attempts to allocate a usable address within the IA_NA address prefix range to the client upon receiving the IA_NA address request from the client. That address will be allocated to other clients if the client no longer uses that address again.	
Configuration Examples	The following example sets the IA_NA address prefix for the DHCPv6 Server.	
	FS(config-dhcp)# iana-address prefix 2008:50::/64 lifetime 2000 1000	

Related Commands	Command	Description
	ipv6 dhcp pool	Sets the DHCPv6 pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.
Platform Description	N/A	

5.9 ipv6 dhcp client ia

	Use this command to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server. Use the no form of this command to restore the default setting.	
	ipv6 dhcp client ia [rapid-commit]	
	no ipv6 dhcp client ia	
Parameter Description	Parameter	Description
	rapid-commit	Allows the two-message interaction process.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to enable DHCPv6 client mode and request the IANA address from the DHCPv6 server, The rapid-commit key allows the two-message interaction process between the client and the server. After the key is configured, the solicit message transmitted by the client contains the rapid-commit option.	
Configuration Examples	The following example enables the request for the IANA address on the interface. <pre>FS(config)# interface fastethernet 0/1 FS(config-if)# ipv6 dhcp client ia</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.10 ipv6 dhcp client pd

	Use this command to enable the DHCPv6 client and request for the prefix address information. Use the no form of this command to restore the default setting.	
	ipv6 dhcp client pd <i>prefix-name</i> [rapid-commit]	
	no ipv6 dhcp client pd	

Parameter	Parameter	Description
Description	prefix-name	Defines the IPv6 prefix name.
	rapid-commit	Allows the two-message interaction process.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	With the DHCPv6 client mode disabled, use this command to enable the DHCPv6 client mode on the interface. With the ipv6 dhcp client pd command enabled, the DHCPv6 client sends the prefix request to the DHCPv6 server The keyword rapid-commit allows the client and the server two-message interaction process. With this keyword configured, the solicit message sent by the client includes the rapid-commit item.	
Configuration Examples	The following example enables the prefix information request on the interface. <pre>FS(config)# interface fastethernet 0/1 FS(config-if)# ipv6 dhcp client pd pd_name</pre>	
Related Commands	Command	Description
	clear ipv6 dhcp client	Resets the DHCPv6 client function on the interface.
	show ipv6 dhcp interface	Displays the DHCPv6 interface configuration.
Platform Description	N/A	

5.11 ipv6 dhcp pool

	Use this command to set the DHCPv6 server pool. Use the no form of this command to restore the default setting.	
	ipv6 dhcp pool <i>poolname</i>	
	no ipv6 dhcp pool <i>poolname</i>	
Parameter	Parameter	Description
Description	poolname	Defines the DHCPv6 pool name.
Defaults	By default, no DHCPv6 server pool is configured.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to create a DHCPv6 Server configuration pool. After configuring this command, it enters the DHCPv6 pool configuration mode, in which the administrator can set the pool parameters, such as the prefix and the DNS Server information, ect.	

	After creating the DHCPv6 Server configuration pool, use the ipv6 dhcp server command to associate the pool and the DHCPv6 Server on one interface.	
Configuration Examples	The following example sets the DHCPv6 server pool. FS# configure terminal FS(config)# ipv6 dhcp pool pool1 FS(config-dhcp)#	
Related Commands	Command	Description
	ipv6 dhcp server	Enables the DHCPv6 server function on the interface.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.
Platform Description	N/A	

5.12 ipv6 dhcp relay destination

	Use this command to enable the DHCPv6 relay service and configure the destination address to which the messages are forwarded. Use the no form of this command to restore the default setting.	
	ipv6 dhcp relay destination <i>ipv6-address [interface-type interface-number]</i>	
	no ipv6 dhcp relay destination <i>ipv6-address [interface-type interface-number]</i>	
Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Sets the DHCPv6 relay destination address.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Specifies the forwarding output interface if the forwarding address is the local link address.
Defaults	By default, the relay and forward function is disabled, and the forwarding destination address and the output interface are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	With the DHCPv6 relay service enabled on the interface, the DHCPv6 message received on the interface can be forwarded to all configured destination addresses. Those received DHCPv6 messages can be from the client, or from another DHCPv6 relay service. The forwarding output interface configuration is mandatory if the forwarding address is the local link address or the multicast address. And the forwarding output interface configuration is optional if the forwarding address is global or station unicast or multicast address. Without the forwarding output interface configured, the interface is selected according to the unicast or multicast routing protocol. The relay reply message can be forwarded without the relay function enabled on the interface.	

Configuration Examples	The following example enables DHCPv6 Relay and sets the relay destination address on the interface to 3001::2.	
	<pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# interface vlan 1 FS(config-if)# ipv6 dhcp relay destination 3001::2 FS(config-if)# end</pre>	
Related Commands	Command	Description
	show ipv6 dhcp interface	Displays the DHCPv6 interface information.
Platform Description	N/A	

5.13 ipv6 dhcp server

	Use this command to enable the DHCPv6 server on the interface. Use the no form of this command to restore the default setting.	
	ipv6 dhcp server <i>poolname</i> [rapid-commit] [preference value]	
	no ipv6 dhcp server	
Parameter Description	Parameter	Description
	poolname	Defines the DHCPv6 pool name.
	rapid-commit	Allows the two-message interaction process.
	preference value	Sets the preference level for the advertise message. The valid range is from 1 to 100 and the default value is 0.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use the ipv6 dhcp server command to enable the DHCPv6 service. Configuring the keyword rapid-commit allows the two-message interaction for the server and the client when allocating the address prefix and setting other configurations. With this keyword configured, if the client solicit message includes the rapid-commit item, the DHCPv6 Server will send the Reply message immediately. DHCPv6 Server carries with the preference value when sending the advertise message if the preference level is not 0. If the preference level is 0, the advertise message will not include this field. If the preference value is 255, the client sends the request message to the server to obtain the configurations. DHCPv6 Client, Server and Relay functions are exclusive, and only one of the functions can be configured on the interface.	
Configuration Examples	The following example enables the DHCPv6 server on the interface.	
	<pre>FS(config)# interface fastethernet 0/1</pre>	

	FS(config-if)# ipv6 dhcp server pool1	
Related Commands	Command	Description
	ipv6 dhcp pool	Sets the DHCPv6 pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.
Platform	N/A	
Description		

5.14 ipv6 local pool

	Use this command to configure the local prefix pool of the DHCPv6 server prefix. Use the no form of this command to restore the default setting.	
	ipv6 local pool <i>poolname prefix/prefix-length assigned-length</i>	
	no ipv6 local pool <i>poolname</i>	
Parameter Description	Parameter	Description
	<i>poolname</i>	The local prefix pool name
	<i>prefix/prefix-length</i>	The prefix and prefix length
	<i>assigned-length</i>	The assigned prefix length
Defaults	By default, no local prefix pool of the DHCPv6 server prefix is configured.	
Command Mode	Global configuration mode	
Usage Guide	The ipv6 local pool command is used to create the local prefix pool. If the DHCPv6 server requires prefix delegation, you can use the prefix-delegation pool command to specify the local prefix pool and then assign prefixes from the prefix pool.	
Configuration Examples	The following example configures the local prefix pool.	
	FS(config)# ipv6 local pool client-prefix-pool 2001::db8::/64 80	
	The following example specifies the local prefix pool.	
	FS(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

5.15 option52

	Use this command to configure the DHCPv6 Server to set the CAPWAP AC IPv6 address.

	Use the no form of this command to restore the default setting.	
	option52 <i>ipv6-address</i>	
	no option52 <i>ipv6-address</i>	
Parameter	Parameter	Description
Description	<i>ipv6-address</i>	Sets the CAPWAP AC IPv6 address.
Defaults	By default, no option52 is created after pool configuration on the DHCPv6 server is complete.	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	This command can be used to set multiple CAPWAP AC IPv6 addresses. The newly added IPv6 address does not overwrite the old one.	
Configuration Examples	The following example configures the domain-name address. FS(config-dhcp)# option52 2008:1::1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.16 prefix-delegation

	Use this command to set the static binding address prefix information for the DHCPv6 server.	
	Use the no form of this command to restore the default setting.	
	prefix-delegation <i>ipv6-prefix/prefix-length client-DUID [lifetime]</i>	
	no prefix-delegation <i>ipv6-prefix/prefix-length client-DUID [lifetime]</i>	
Parameter	Parameter	Description
Description	<i>ipv6-prefix/prefix-length</i>	Sets the IPv6 address prefix and the prefix length.
	<i>client-DUID</i>	Sets the client DUID.
	<i>lifetime</i>	Sets the interval of using the prefix by the client.
Defaults	By default, no address prefix information is configured. The default <i>lifetime</i> is 3,600 seconds (one hour).	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	The administrator uses this command to manually set the address prefix information list for the client IA_PD and set the valid lifetime for those prefixes.	

	The parameter <i>client-DUID</i> allocates the address prefix to the first IA_PD in the specified client. Before receiving the request message for the address prefix from the client, DHCPv6 Server searches for the corresponding static binding first. If it succeeds, the server returns to the static binding; otherwise, the server will attempt to allocate the address prefix from other prefix information sources.	
Configuration Examples	The following example sets the prefix information for a DHCPv6 client. <pre>FS(config-dhcp)# prefix-delegation 2008:2::/64 0003000100d0f82233ac</pre>	
Related Commands	Command	Description
	ipv6 dhcp pool	Sets a DHCPv6 pool.
	ipv6 local pool	Sets a local prefix pool.
	prefix-delegation pool	Specifies the DHCPv6 local prefix pool.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.
Platform Description	N/A	

5.17 prefix-delegation pool

	Use this command to specify the local prefix pool for the DHCPv6 server. Use the no form of this command to restore the default setting.	
	prefix-delegation pool <i>poolname</i> [lifetime { <i>valid-lifetime</i> <i>preferred-lifetime</i> }]	
	no prefix-delegation pool <i>poolname</i>	
Parameter Description	Parameter	Description
	<i>poolname</i>	Sets the local prefix pool name.
	lifetime	Sets the lifetime of the address prefix allocated to the client. With the keyword lifetime configured, both parameters <i>valid-lifetime</i> and <i>preferred-lifetime</i> shall be configured.
	<i>valid-lifetime</i>	Sets the valid lifetime of using the allocated address prefix for the client.
	<i>preferred-lifetime</i>	Sets the preferred lifetime of the address prefix allocated to the client.
Defaults	By default, no address prefix pool is specified. The default <i>valid-lifetime</i> is 3,600s(1 hour). The default <i>preferred-lifetime</i> is 3,600s(1 hour).	
Command Mode	DHCPv6 pool configuration mode	
Usage Guide	Use the prefix-delegation pool command to set the prefix pool for the DHCPv6 Server and allocate the prefix to the client. Use the ipv6 local pool command to set the prefix pool. The Server attempts to allocate a usable prefix from the prefix pool to the client upon receiving the prefix request from the client. That prefix will be allocated to other clients if the client no longer uses that prefix again.	

Configuration	The following example specifies the local prefix pool for the DHCPv6 server.	
Examples	FS(config-dhcp)# prefix-delegation pool client-prefix-pool lifetime 2000 1000	
Related Commands	Command	Description
	ipv6 dhcp pool	Sets a DHCPv6 pool.
	ipv6 local pool	Sets a local prefix pool.
	prefix-delegation	Statically binds the client with the address prefix.
	show ipv6 dhcp pool	Displays the DHCPv6 pool information.
Platform	N/A	
Description		

5.18 show ipv6 dhcp

	Use this command to display the device DUID.	
	show ipv6 dhcp	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Interface configuration mode/Global configuration mode	
Usage Guide	The server, client and relay on the same device share a DUID.	
Configuration	The following example displays the device DUID.	
Examples	FS# show ipv6 dhcp This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

5.19 show ipv6 dhcp binding

	Use this command to display the address binding information for the DHCPv6 server.	
	show ipv6 dhcp binding [ipv6-address]	
Parameter	Parameter	Description
Description	ipv6-address	Sets the IPv6 address or the prefix.

Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	If the <i>ipv6-address</i> is not specified, all prefixes dynamically assigned to the client and IANA address binding information are shown. If the <i>ipv6-address</i> is specified, the binding information for the specified address is shown.				
Configuration Examples	The following example displays the address binding information for the DHCPv6 server. <pre> FS# show ipv6 dhcp binding Client DUID: 00:03:00:01:00:d0:f8:22:33:ac IAPD: iaid 0, T1 1800, T2 2880 Prefix: 2001:20::/72 preferred lifetime 3600, valid lifetime 3600 expires at Jan 1 2008 2:23 (3600 seconds) </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

5.20 show ipv6 dhcp conflict

	Use this command to display the DHCPv6 address conflicts.	
	show ipv6 dhcp conflict	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the DHCPv6 address conflicts. FS# show ipv6 dhcp conflict 2008:50::2 declined 2108:50::2 declined 2008:50::3 declined 2008:50::4 declined	

	2108:50::4	declined
	2008:50::5	declined
Related Commands	Command	
	Description	
	clear ipv6 dhcp conflict	Clears address conflicts.
Platform Description	N/A	

5.21 show ipv6 dhcp interface

	Use this command to display the DHCPv6 interface information.	
	show ipv6 dhcp interface [<i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Sets the interface name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If the <i>interface-name</i> is not specified, all DHCPv6 interface information is displayed. If the <i>interface-name</i> is specified, the specified interface information is displayed.	
Configuration Examples	The following example displays the DHCPv6 interface information. <pre>FS# show ipv6 dhcp interface VLAN 1 is in server mode Server pool dhcp-pool Rapid-Commit: disable</pre>	
Related Commands	Command	
	Description	
	N/A	N/A
Platform Description	N/A	

5.22 show ipv6 dhcp pool

	Use this command to display the DHCPv6 pool information.	
	show ipv6 dhcp pool [<i>poolname</i>]	
Parameter Description	Parameter	Description
	<i>poolname</i>	Defines the DHCPv6 pool name.

Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	If the <i>poolname</i> is not specified, all DHCPv6 interface information is displayed. If the <i>poolname</i> is specified, the specified interface information is displayed.				
Configuration Examples	The following example displays the DHCPv6 pool information. <pre>FS# show ipv6 dhcp pool DHCPv6 pool: dhcp-pool DNS server: 2011:1::1 DNS server: 2011:1::2 Domain name: example.com</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

5.23 show ipv6 dhcp relay destination

	Use this command to display the destination information about DHCPv6 Relay Agent.	
	show ipv6 dhcp relay destination { all interface-type interface-number }	
Parameter description	Parameter	Description
	all	Displays information about all configured destination addresses and relay exits.
	interface-type interface-number	Displays the relay destination address and relay exit configured for a specified interface.
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage guideline	Use this command to show the relay destination address to which DHCPv6 packets sent from a client are forwarded through a specified relay exit (optional) by an interface for which the relay function has been enabled by Relay Agent.	
Examples	The following example displays all the relay destination addresses. <pre>FS# show ipv6 dhcp relay destination all</pre>	

	Interface:VLAN 1	
	Destination address(es)	Output Interface
	3001::2	
	ff02::1:2	VLAN 2
Related commands	Command	Description
	N/A	N/A
Platform description	N/A	

5.24 show ipv6 dhcp relay statistics

	Use this command to display the packet sending and receiving condition with the DHCPv6 Relay function enabled.	
	show ipv6 dhcp relay statistics	
Parameter	Parameter	Description
Description	N/A.	N/A.
Defaults	N/A.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A.	

Configuration Examples	The following example displays the packet sending and receiving condition with the DHCPv6 Relay function enabled.	
	<pre>FS# show ipv6 dhcp relay statistics Packets dropped : 2 Error : 2 Excess of rate limit : 0 Packets received : 28 SOLICIT : 0 REQUEST : 0 CONFIRM : 0 RENEW : 0 REBIND : 0 RELEASE : 0 DECLINE : 0 INFORMATION-REQUEST : 14 RELAY-FORWARD : 0 RELAY-REPLY : 14 Packets sent : 16 ADVERTISE : 0 RECONFIGURE : 0 REPLY : 8 RELAY-FORWARD : 8 RELAY-REPLY : 0</pre>	
Related Commands	Command	Description
	clear ipv6 dhcp relay statistics	Clears the statistical information.
Platform Description	N/A	

5.25 show ipv6 dhcp server statistics

	Use this command to display the DHCPv6 server statistics.	
	show ipv6 dhcp server statistics	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the DHCPv6 server statistics.	

Configuration	The following example displays the DHCPv6 server statistics.	
Examples	<pre> FS# show ipv6 dhcp server statistics DHCPv6 server statistics: Packet statistics: DHCPv6 packets received: 7 Solicit received: 7 Request received: 0 Confirm received: 0 Renew received: 0 Rebind received: 0 Release received: 0 Decline received: 0 Relay-forward received: 0 Information-request received: 0 Unknown message type received: 0 Error message received: 0 DHCPv6 packet sent: 0 Advertise sent: 0 Reply sent: 0 Relay-reply sent: 0 Send reply error: 0 Send packet error: 0 Binding statistics: Bindings generated: 0 IAPD assigned: 0 IANA assigned: 0 Configuration statistics: DHCPv6 server interface: 1 DHCPv6 pool: 0 DHCPv6 iapd binding: 0 </pre>	
Related	Command	Description
Commands	ipv6 dhcp pool	Sets a DHCPv6 pool.
Platform	N/A	
Description		

5.26 show ipv6 local pool

	Use this command to display the local prefix pool configuration and usage.																	
	show ipv6 local pool [<i>poolname</i>]																	
Parameter	Parameter	Description																
Description	<i>poolname</i>	The local prefix pool name																
Defaults	N/A																	
Command Mode	Privileged EXEC mode																	
Usage Guide	This command is used to display the local prefix pool configuration and usage.																	
Configuration Examples	The following example displays all local prefix pool information. <pre>FS#show ipv6 local pool Pool Free In use client-prefix-pool 2001:db8::/64 65536 0</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Pool</td><td>The local address pool name.</td></tr><tr><td>Prefix</td><td>The prefix and prefix length.</td></tr><tr><td>Free</td><td>The available prefix.</td></tr><tr><td>In use</td><td>The prefix in use.</td></tr></table> The following example displays the information about the specified local prefix pool. <pre>FS#show ipv6 local pool client-prefix-pool Prefix is 2001:db8::/64 assign /80 prefix 1 entries in use, 65535 available Prefix Interface 2001:db8::/80 GigabitEthernet 0/0</pre> <table><tr><th>Filed</th><th>Description</th></tr><tr><td>Prefix</td><td>The assigned prefix and prefix length.</td></tr><tr><td>Interface</td><td>The assigning interface.</td></tr></table>		Field	Description	Pool	The local address pool name.	Prefix	The prefix and prefix length.	Free	The available prefix.	In use	The prefix in use.	Filed	Description	Prefix	The assigned prefix and prefix length.	Interface	The assigning interface.
Field	Description																	
Pool	The local address pool name.																	
Prefix	The prefix and prefix length.																	
Free	The available prefix.																	
In use	The prefix in use.																	
Filed	Description																	
Prefix	The assigned prefix and prefix length.																	
Interface	The assigning interface.																	
Related Commands	Command	Description																
	N/A	N/A																
Platform Description	N/A																	

6 DNS Commands

6.1 clear host

	Use this command to clear the dynamically learned host name.	
	clear host [* <i>host-name</i>]	
Parameter Description	Parameter	Description
	host-name	Deletes the specified dynamic domain name buffer.
	*	Deletes all dynamic domain name buffer.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	You can obtain the mapping record of the host name buffer table in two ways: 1) the ip host static configuration, 2) the DNS dynamic learning. Execute this command to delete the host name records learned by the DNS dynamically.	
Configuration Examples	The following configuration deletes the dynamically learned mapping records from the host name-IP address buffer table.	
	FS(config)#clear host *	
Related Commands	Command	Description
	show hosts	Displays the host name buffer table.
Platform Description	N/A	

6.2 ip domain-lookup

	Use this command to enable DNS domain name resolution. Use the no form of this command to disable the DNS domain name resolution function. Use the default form of this command to restore the default settings.	
	ip domain-lookup	
	no ip domain-lookup	
	default ip domain-lookup	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is enabled by default.				
Command Mode	Global configuration mode.				
Usage Guide	N/A				
Configuration Examples	The following example disables the DNS domain name resolution function. FS(config)# no ip domain-lookup				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show hosts</td><td>Displays the DNS related configuration information.</td></tr> </table>	Command	Description	show hosts	Displays the DNS related configuration information.
Command	Description				
show hosts	Displays the DNS related configuration information.				
Platform Description	N/A				

6.3 ip host

	Use this command to configure the mapping of the host name and the IP address. Use the no form of the command to remove the host list.	
	ip host <i>host-name ip-address</i>	
	no ip host <i>host-name ip-address</i>	
Parameter Description	Parameter	Description
	host-name	The host name of the equipment
	ip-address	The IP address of the equipment
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures IPv4 address 192.168.5.243 for domain name www.test.com. FS(config)# ip host www.test.com 192.168.5.243	
Related Commands	Command	Description
	show hosts	Show the DNS related configuration information.

Platform	N/A
Description	

6.4 ip name-server

	Use this command to configure the IP address of the domain name server. Use the no form of this command to delete the configured domain name server.	
	ip name-server [oob] { <i>ip-address</i> <i>ipv6-address</i> } [via <i>mgmt-name</i>]	
	no ip name-server [oob] { <i>ip-address</i> <i>ipv6-address</i> } [via <i>mgmt-name</i>]	
Parameter Description	Parameter	Description
	oob	Enables the out-band channel. It must be set when MGMT is specified as the source port.
	ip-address	The IP address of the domain name server.
	ipv6-address	The IPv6 address of the domain name server.
	via	Configures MGMT port.
	mgmt-name	Specifies the MGMT port in oob mode.
Defaults	No domain name server is configured by default.	
Command Mode	Global configuration mode.	
Usage Guide	Add the IP address of the DNS server. Once this command is executed, the equipment will add a DNS server. When the device cannot obtain the domain name from a DNS server, it will attempt to send the DNS request to subsequent servers until it receives a response. Up to 6 DNS servers are supported. You can delete a DNS server with the <i>ip-address</i> option or all the DNS servers.	
Configuration Examples	The following example configures the IPv4 and IPv6 DNS servers. <pre>FS(config)# ip name-server 192.168.5.134 via mgmt 2/0 FS(config)# ip name-server 2001:0DB8::250:8bff:fee8:f800 2001:0DB8:0:f004::1 via mgmt 2/0</pre>	
Related Commands	Command	Description
	show hosts	Displays the DNS related configuration information.
Platform Description	N/A	

6.5 ipv6 host

	Use this command to configure the mapping of the host name and the IPv6 address by manual. Use the no form of the command to remove the host list.

	ipv6 host <i>host-name ipv6-address</i>	
	no ipv6 host <i>host-name ipv6-address</i>	
Parameter Description	Parameter	Description
	host-name	The host name of the equipment
	ipv6-address	The IPv6 address of the equipment
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	To delete the host list, use the no ipv6 host <i>host-name ipv6-address</i> command.	
Configuration Examples	The following example configures the IPv6 address for the domain name. FS(config)# ipv6 host switch 2001:0DB8:700:20:1::12	
Related Commands	Command	Description
	show hosts	Displays the DNS related configuration information.
Platform Description	N/A	

6.6 show hosts

	Use this command to display DNS configuration.	
	show hosts [<i>hostname</i>]	
Parameter Description	Parameter	Description
	<i>hostname</i>	Displays the specified domain name information,
Defaults	All domain name information is displayed by default.	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command is used to display the DNS related configuration information.	
Configuration Examples	FS# show hosts Name servers are: 192.168.5.134 static	

	Host	type	Address	TTL(sec)	
	switch	static	192.168.5.243	---	
	www.FS.com	dynamic	192.168.5.123	126	
	Field			Description	
	Name servers			Domain name server	
	Host			Domain name	
	type			Resolution type: Static resolution and dynamic resolution.	
	Address			IP address corresponding to the domain name	
	TTL			TTL of entries corresponding to the domain name/IP address.	
	Related Commands	Command			Description
		ip host			Configures the host name and IP address mapping by manual.
		ipv6 host			Configures the host name and IPv6 address mapping by manual.
		ip name-server			Configures the DNS server.
Platform Description	N/A				

7 FTP Server Commands

7.1 ftp-server enable

	Use this command to enable the FTP server. Use the default form of this command to restore the default setting.	
	ftp-server enable	
	default ftp-server enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable the FTP server to connect the FTP client to upload/download the files.  To enable the FTP client to access to the FTP server files, this command shall be co-used with the ftp-server topdir command.	
Configuration Examples	The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory: <pre>FS(config)# ftp-server topdir /syslog FS(config)# ftp-server enable</pre> The following example disables the FTP Server: <pre>FS(config)# no ftp-server enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.2 ftp-server login timeout

	Use this command to set the timeout interval for login to the FTP server. Use the no or default form of this command to restore the default setting.	
	ftp-server login timeout <i>time</i>	
	no ftp-server login timeout	
	default ftp-server login timeout	

Parameter Description	Parameter	Description
	<i>time</i>	Sets the timeout interval for login to the FTP server, in the range from 1 to 30 in the unit of minutes.
Defaults	The default is 2 minutes.	
Command Mode	Global configuration mode	
Usage Guide	The timeout interval refers to the maximum time when your account is allowed online after you login to the server. If you don't perform authentication again before the timeout interval expires, you will be forced offline.	
Configuration Examples	The following example sets the timeout interval for login to the FTP server to 5 minutes. <pre>FS(config)# ftp-server login timeout 5</pre> The following example restores the default setting. <pre>FS(config)# no ftp-server login timeout</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.3 ftp-server login times

	Use this command to set the number of login attempts. Use the no or default form of this command to restore the default setting.	
	ftp-server login times <i>time</i>	
	no ftp-server login times	
	default ftp-server login times	
Parameter Description	Parameter	Description
	<i>time</i>	Sets the number of login attempts, in the range from 1 to 10.
Defaults	The default is 3.	
Command Mode	Global configuration mode	

Usage Guide	The number of login attempts refers to the maximum count you are allowed to perform authentication. If the number of your login attempts exceeds 3, you will be forced offline.	
Configuration Examples	The following example sets the number of login attempts to 5. <pre>FS(config)# ftp-server login times 5</pre> The following example restores the default setting. <pre>FS(config)# no ftp-server login times</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.4 ftp-server timeout

	Use this command to set the FTP session idle timeout. Use the no or default form of this command to restore the default setting.	
	ftp-server timeout <i>time</i>	
	no ftp-server timeout	
	default ftp-server timeout	
Parameter Description	Parameter	Description
	<i>time</i>	Sets the session idle timeout, in the range from 1 to 3600 in the unit of minutes.
Defaults	The default is 10 minutes.	
Command Mode	Global configuration mode.	
Usage Guide	Use this command to set the FTP session idle timeout. If the session is idle, the FTP server deems the session connection is invalid and disconnects with the user.  The session idle time refers to the time for the FTP session between two FTP operations.	
Configuration Examples	The following example sets the session idle timeout to 5 minutes: <pre>FS(config)# ftp-server timeout 5</pre> The following example restores the default setting. <pre>FS(config)# no ftp-server timeout</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.5 ftp-server topdir

	Use this command to set the directory range for the FTP client to access to the FTP server files. Use the no or default form of this command to restore the default setting.	
	ftp-server topdir <i>directory</i>	
	no ftp-server topdir	
	default ftp-server topdir	
Parameter Description	Parameter	Description
	<i>directory</i>	Sets the top-directory.
Defaults	No top-directory is configured by default.	
Command Mode	Global configuration mode.	
Usage Guide	The FTP server top directory specifies the directory range of the files accessed by the client. Can the FTP client accesses to the files on the FTP server with the top directory correctly specified. Without this command configured, FTP client fails to access to any file or directory on the FTP server.	
Configuration Examples	The following example enables the FTP Server and confines the FTP client access to the syslog subdirectory. <pre>FS(config)# ftp-server topdir /syslog FS(config)# ftp-server enable</pre> The following example restores the default setting. <pre>FS(config)# no ftp-server topdir</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.6 ftp-server username password

	Use this command to set the login username and password for the FTP server. Use the no form of this command to restore the default setting.	
	ftp-server username <i>username</i> password [<i>type</i>] <i>password</i>	
	no ftp-server username <i>username</i>	
	default ftp-server username <i>username</i>	
Parameter Description	Parameter	Description
	<i>username</i>	Sets the login username.
	<i>password</i>	Sets the log password
Defaults	No username or password is set by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the login username for the FTP server. To log in to the FTP server, the correct username and password shall be provided. The maximum length of the username is 64 characters and the spaces are not allowed in the middle of the username. The username consists of letters, semiangle number and semiangle mark. Ten usernames can be configured for the FTP server at most. The password must contain letters or numbers. Spaces before or behind the password are allowed but will be ignored. The spaces within are part of the password. The plaintext password is in the range from 1 to 25 characters. The encrypted password is in the range from 4 to 52 characters.  The anonymous user login is not supported on the FTP server. The client fails to pass the identity verification if the username is removed.	
Configuration Examples	The following example sets the username to user: <pre>FS(config)# ftp-server username user password pass</pre> The following example restores the default setting: <pre>FS(config)# no ftp-server username user</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 show ftp-server

	Use this command to show the status information of the FTP server.	
	show ftp-server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	The FTP server status information includes: ● Enabled/Disabled server ● The FTP server top directory ● The FTP server user information, including username, password and connection number. If connection is set up, the IP address, port, transmission type, active/passive mode is shown	
Configuration Examples	The following example displays the related status information of the FTP server: <pre> FS#show ftp-server ftp-server information ===== enable : Y topdir : tmp:/ timeout: 10min username:aaaa password:(PLAIN)bbbb connect num[2] [0]trans-type:BINARY (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3927] [1]trans-type:ASCII (ctrl)server IP:192.168.21.100[21] client IP:192.168.21.26[3929] username:a1 password:(PLAIN)bbbb connect num[0] username:a2 password:(PLAIN)bbbb connect num[0] username:a3 password:(PLAIN)bbbb connect num[0] username:a4 password:(PLAIN)bbbb connect num[0] username:a5 password:(PLAIN)bbbb connect num[0] </pre>	

	username:a6	password:(PLAIN)bbbb	connect num[0]
	username:a7	password:(PLAIN)bbbb	connect num[0]
	username:a8	password:(PLAIN)bbbb	connect num[0]
	username:a9	password:(PLAIN)bbbb	connect num[0]
Related Commands	Command		Description
	N/A		N/A
Platform Description	N/A		

8 FTP CLIENT Commands

8.1 copy flash

	Use this command to upload the file from the server to the device through FTP Client.	
	copy flash: <i>[local-directory/] local-file ftp://username:password@dest-address [/remote-directory] / remote-file</i>	
Parameter Description	Parameter	Description
	username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	dest-address	IP address of the target FTP Server.
	remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
	remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
	local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
	local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples	The following example uploads the file named "local-file" in directory "home" of local device to directory "root" on the FTP Server whose user name is user, password is pass and IP address is 192.168.23.69, and changes the filename to "remote-file". <pre>FS# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.2 copy ftp

	Use this command to download the file from the server to the device through FTP Client.	
	copy ftp://username:password@dest-address [/remote-directory] / remote-file flash:[local-directory/] local-file	
Parameter Description	Parameter	Description
	username	The username for logging into FTP Server. It is limited to 40 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	password	The password for logging into FTP Server. It is limited to 32 bytes and must not contain ":", "@", "/" and space, neither can it be omitted.
	dest-address	IP address of the target FTP Server.
	remote-directory	File directory of FTP Server. It is optional and limited to 255 bytes. No space or Chinese character is supported. If left blank, it implies the current directory of FTP server.
	remote-file	Filename on the remote server. It is limited to 255 bytes and doesn't support space or Chinese character.
	local-directory	Directory of local folder (optional). If this directory is specified, this directory must have been created beforehand. This command doesn't support automatic directory creation. If left blank, it implies the current directory on the local device. It is limited to 255 bytes and doesn't support space or Chinese characters.
	local-file	Filename on the local device. It is limited to 255 bytes and doesn't support space or Chinese character.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A	
Configuration Examples	The following example uses username of "user" and password of "pass" to download a file named "remote-file" from the directory "root" on FTP Server with IP address 192.168.23.69 to directory "home" on the local device, and changes the name to "local-file". <pre>FS# copy ftp://user:pass@192.168.23.69/root/remote-file flash:home/local-file</pre> The following example uploads a file named "local-file" from directory "home" on the local device to directory "root" on FTP Server, and changes the name to "remote-file". <pre>FS# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file</pre>	
Related Commands	Command	Description
	copy tftp	Uses the TFTP protocol to transfer files.
Platform Description	N/A	

8.3 ftp-client ascii

	Use this command to use ASCII mode for FTP transfer. Use the no or default form of this command to restore the default setting.	
	ftp-client [vrf vrfname] ascii	
	no ftp-client [vrf vrfname] ascii	
	default ftp-client [vrf vrf-name]	
Parameter Description	Parameter	Description
	vrf vrf-name	Configures the file transfer mode for the specified VRF.
Defaults	The default FTP transfer mode is binary.	
Command Mode	Global configuration mode	
Usage Guide	The default command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.	
Configuration Examples	The following example configures ASCII FTP transfer. <pre>FS (config)# ftp-client ascii</pre> The following example configures ASCII FTP transfer for <i>vrf-name</i>. <pre>FS(config)# ftp-client vrf vrf-name ascii</pre> The following example configures binary FTP transfer.	

	<pre>FS(config)# no ftp-client ascii</pre> The following example configures binary FTP transfer for <i>vrf-name</i>. <pre>FS(config)# no ftp-client vrf vrf-name ascii</pre> The following example restores the default setting of the FTP Client. <pre>FS(config)# default ftp-client</pre> The following example restores the default setting of the FTP Client vrf-name, <pre>FS(config)# default ftp-client vrf vrf-name</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.4 ftp-client port

	Use this command to configure PORT mode used for FTP data connection. Use the no or default form of this command to restore the default setting.	
	ftp-client [vrf vrf-name] port	
	no ftp-client [vrf vrf-name] port	
	default ftp-client [vrf vrf-name]	
Parameter Description	Parameter	Description
	vrf vrf-name	VRF name The default is the public network instance.
Defaults	The default is PASV mode for FTP data connection.	
Command Mode	Global configuration mode.	
Usage Guide	This command is used to configure the connection mode to PORT mode, in which the server will actively connect with the client. The default command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound.	
Configuration Examples	The following example configures PORT mode used for FTP data connection <pre>FS (config)# ftp-client port</pre> The following example configures PORT mode used for FTP <i>vrf-name</i> data connection. <pre>FS(config)# ftp-client vrf vrf-name port</pre> The following example configures PASV mode for FTP data connection. <pre>FS(config)# no ftp-client port</pre> The following example configures PASV mode used for FTP <i>vrf-name</i> data connection.	

	<pre>FS(config)# no ftp-client vrf vrf-name port</pre> The following example restores the default setting of the FTP Client. <pre>FS(config)# default ftp-client</pre> The following example restores the default setting of the FTP Client vrf-name, <pre>FS(config)# default ftp-client vrf vrf-name</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.5 ftp-client source

	Use this command to bind FTP Client with the source IP address of client and use this IP address to communicate with server. Use the no form of this command to disable source IP address binding. Use the default form of this command to restore the default setting.	
	ftp-client [vrf <i>vrf-name</i>] source { <i>ip-address</i> <i>ipv6-address</i> <i>interface</i> }	
	no ftp-client [vrf <i>vrf-name</i>] source	
	default ftp-client [vrf <i>vrf-name</i>]	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	VRF name. The default is the public network instance.
Defaults	By default, the IP address is not bound with the client locally. Instead, it is selected by the route.	
Command Mode	Global configuration mode	
Usage Guide	The default command is used to restore the FTP client setting. Specifically, data connection is in PASV mode and file transfer BINARY. The client source IP address is not bound. The ftp-client [vrf <i>vrfname</i>] source-address {<i>ip-address</i> <i>ipv6-address</i>} command will be converted to this command automatically	
Configuration Examples	The following example binds FTP Client with source IP address 192.168.23.236. <pre>FS(config)# ftp-client source 192.168.23.236</pre> The following example binds FTP Client with source IP address 2003:0:0:0::2. <pre>FS(config)# ftp-client source 2003:0:0:0::2</pre> The following example binds FTP Client <i>vrf-name</i> with source IP address 192.168.23.236. <pre>FS(config)# ftp-client vrf vrf-name source 192.168.23.236</pre> The following example binds FTP Client <i>vrf-name</i> with source IP address 2003:0:0:0::2. <pre>FS(config)# ftp-client vrf vrf-name source 2003:0:0:0::2</pre>	

	The following example disables source IP address binding. <pre>FS(config)# no ftp-client source</pre> The following example disables source IP address binding. <pre>FS(config)# no ftp-client vrf vrf-name source</pre> The following example restores the default setting of the FTP Client. <pre>FS(config)# default ftp-client</pre> The following example restores the default setting of the FTP Client vrf-name, <pre>FS(config)# default ftp-client vrf vrf-name</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9 TFTP Server Commands

9.1 tftp-server enable

	Use this command to enable the TFTP server. Use the no form of this command to disable the TFTP server.	
	tftp-server enable	
	no tftp-server enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The TFTP server is disabled by default.	
Command Modes	Global configuration mode	
Usage Guide	Only with the TFTP server enabled and the top directory configured meanwhile, TFTP clients are able to upload or download files.	
Configuration Examples	The following example enables the TFTP server and sets the top directory of the TFTP server to /syslog. <pre>FS(config)# tftp-server topdir /syslog FS(config)# tftp-server enable</pre> The following example disables the TFTP server. <pre>FS(config)# no tftp-server enable</pre>	
Platform Description	N/A	

9.2 tftp-server topdir

	Use this command to configure the top directory for TFTP clients. Use the no or default form of this command to restore the default setting.	
	tftp-server topdir <i>directory</i>	
	no tftp-server topdir	
	default tftp-server topdir	
Parameter Description	Parameter	Description
	<i>directory</i>	The top directory for TFTP clients to access. "/" means the root directory.

Defaults	By default, the top directory is /flash .
Command Modes	Global configuration mode
Usage Guide	The top directory on the TFTP server defines what files and folders the client is able to access. And the client cannot access the TFTP server before a top directory is correctly configured for the server.
Configuration Examples	The following example enables the TFTP server and sets the top directory for TFTP clients to /syslog. <pre>FS(config)# tftp-server topdir /syslog FS(config)# tftp-server enable</pre> The following example restores the default top directory. <pre>FS(config)# no tftp-server topdir</pre>
Platform Description	N/A

9.3 show tftp-server

	Use this command to display the configuration of the TFTP server.	
	show tftp-server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Modes	Global configuration mode/Privileged configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the progress of downloading the TFTP client. <pre>FS# show tftp-server tftp-server information ===== enable : Y topdir : flash:/</pre>	
Platform Description	N/A	

9.4 show tftp-server updating-list

	Use this command to display the progress of downloading the TFTP client.				
	show tftp-server updating-list				
Parameter Description	Parameter	Description			
	N/A	N/A			
Defaults	N/A				
Command Modes	Global configuration mode/Privileged configuration mode/Interface configuration mode				
Usage Guide	This command is supported only on AM5528 products.				
Configuration Examples	The following example displays the progress of downloading the TFTP client.				
	FS# show tftp-server updating-list				
	IP Address	Interface	File Name	TX	Elapsed
	-----	-----	-----		
	171.208.208.2	GigabitEthernet 0/7	main_map552.bin	6.28392%	00:00:05
Platform Description	N/A				

10 TCP Commands

10.1 ip tcp keepalive

	Use this command to enable the TCP keepalive function. Use the no form of this command to restore the default setting,	
	ip tcp keepalive [interval <i>num1</i>] [times <i>num2</i>] [idle-period <i>num3</i>]	
Parameter Description	Parameter	Description
	interval <i>num1</i>	The interval of sending the keepalive packet, in the range from 1 to 120 in the unit of seconds, The default is 75.
	times <i>num2</i>	Keepalive packet sending times, in the range from 1 to 10. The default is 6.
	idle-period <i>num3</i>	Idle time, the time period during which the peer end does not send any packet to the local end, in the range from 60 to 1800 in the unit of seconds. The default is 900.
Defaults	The function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The keepalive function enables TCP to detect whether the peer end is operating properly. Suppose the keepalive function is enabled together with default interval, times and idle-period settings. TCP begins to send the keepalive packet at an interval of 75 seconds if it does not receive any packet from the peer end in 900 seconds. The TCP connection is considered invalid and then disconnected automatically if the device sends the keepalive packet for six consecutive times without receiving any TCP packet from the peer end. This command applies to both IPv4 and IPv6 TCP.	
Configuration Examples	The following example enables the TCP keepalive function on the device and sets the idle-period and interval to 180 and 60 respectively. If the device sends the keepalive packet for four consecutive times without receiving any TCP packet from the peer end, the TCP connection is considered invalid. <pre>FS(config)# ip tcp keepalive interval 60 times 4 idle-period 180</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.2 ip tcp mss

	Use this command to set the upper limit of the MSS value. Use the no form of this command to restore the default setting.	
	ip tcp mss <i>max-segment-size</i>	
	no ip tcp mss	
Parameter Description	Parameter	Description
	<i>max-segment-size</i>	Upper limit of the MSS value in the range from 68 to 10,000 bytes
Defaults	The default MSS = Outgoing IPv4/v6 MTU- IPv4/v6 header-TCP header.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to limit the maximum value of MSS for the TCP connection to be created. The negotiated MSS cannot exceed the configured value. You can use this command to reduce the maximum value of MSS. However, this configuration is not needed in general. This command applies to both IPv4 and IPv6 TCP.	
Configuration Examples	The following example sets the upper limit of the MSS value to 1,300 bytes. <pre>FS(config)# ip tcp mss 1300</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.3 ip tcp path-mtu-discovery

	Use this command to enable Path Maximum Transmission Unit (PMTU) discovery function for TCP in global configuration mode. Use the no form of this command to restore the default setting.	
	ip tcp path-mtu-discovery [age-timer <i>minutes</i> age-timer infinite]	
	no ip tcp path-mtu-discovery	
Parameter Description	Parameter	Description
	age-timer <i>minutes</i>	The time interval for further discovery after discovering PMTU. Its value ranges from 10 to 30 minutes. The default value is 10.
	age-timer infinite	No further discovery after discovering PMTU
Defaults	This function is disabled by default.	
Command	Global configuration mode	

Mode					
Usage Guide	Based on RFC1191, the TCP path MTU function improves the network bandwidth utilization and data transmission when the user uses TCP to transmit the data in batch. Enabling or disabling this function takes no effect for existent TCP connections and is only effective for TCP connections to be created. This command applies to only IPv4 TCP. This function is enabled for IPv6 TCP constantly and cannot be disabled. According to RFC1191, after discovering the PMTU, the TCP uses a greater MSS to detect the new PMTU at a certain interval, which is specified by the parameter age-timer. If the PMTU discovered is smaller than the MSS negotiated between two ends of the TCP connection, the device will be trying to discover the greater PMTU at the specified interval until the PMTU value reaches the MSS or the user stops this timer. Use the parameter age-timer infinite to stop this timer.				
Configuration Examples	The following example enables PMTU discovery. <pre>FS(config)# ip tcp path-mtu-discovery</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show tcp pmtu</td><td>Shows the PMTU value for the TCP connection.</td></tr> </table>	Command	Description	show tcp pmtu	Shows the PMTU value for the TCP connection.
Command	Description				
show tcp pmtu	Shows the PMTU value for the TCP connection.				
Platform Description	N/A				

10.4 ip tcp send-reset

	Use this command to enable the device to send the reset packet when receiving the TCP port unreachable packet. Use the no form of this command to disable this function,	
	ip tcp send-reset	
	no ip tcp send-reset	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	In general, when dispatching the TCP packet, the TCP module replies a reset packet automatically to disconnect the TCP connection with the peer end if the TCP connection that this packet belongs to is not found. However, flooding TCP port unreachable packets pose an attack threat to the device. This command can be used to disable the device from sending the reset packet when receiving the TCP port unreachable packet. This command applies to both IPv4 and IPv6 TCP.	

Configuration Examples	The following example disables the device from sending the reset packet when receiving the TCP port unreachable packet. FS(config)# no ip tcp send-reset	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.5 ip tcp synwait-time

	Use this command to set the timeout value for SYN packets (the maximum time from SYN transmission to successful three-way handshake). Use the no form of this command to restore the default setting.	
	ip tcp synwait-time <i>seconds</i>	
	no ip tcp synwait-time <i>seconds</i>	
Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout value for SYN packets in the range from 5 to 300 in the unit of seconds.
Defaults	The default is 20.	
Command Mode	Global configuration mode	
Usage Guide	If there is an SYN attack in the network, reducing the SYN timeout value can prevent resource consumption, but it takes no effect for successive SYN attacks. When the device actively requests a connection with an external device, reducing the SYN timeout value can shorten the time for the user to wait, such as telnet login. For poor network conditions, the timeout value can be increased properly. This command applies to both IPv4 and IPv6 TCP.	
Configuration Examples	The following example set the timeout value for SYN packets to 10 seconds. FS(config)# ip tcp syntime-out 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.6 ip tcp window-size

	Use this command to change the size of receiving buffer and sending buffer for TCP connections. Use the no form of this command to restore the default setting.	
	ip tcp window-size <i>size</i>	
	no ip tcp window-size	
Parameter Description	Parameter	Description
	<i>size</i>	Size of receiving buffer and sending buffer for TCP connections in the range from 128 to 65535 << 14 bytes.
Defaults	The default is 65535.	
Command Mode	Global configuration mode	
Usage Guide	The TCP receiving buffer is used to buffer the data received from the peer end. These data will be subsequently read by application programs. Generally, the window size of TCP packets implies the size of free space in the receiving buffer. For connections involving a large bandwidth and mass data, increasing the size of receiving buffer will remarkably improve TCP transmission performance.	
Configuration Examples	The following example sets the TCP window size to 16386 bytes. FS(config)# ip tcp window-size 16386	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.7 show ipv6 tcp connect

	Use this command to display the current IPv6 TCP connection information.	
	show ipv6 tcp connect [local-ipv6 <i>X:X:X:X::X</i>] [local-port <i>num</i>] [peer-ipv6 <i>X:X:X:X::X</i>] [peer-port <i>num</i>]	
	Use this command to display the current IPv6 TCP connection statistics.	
	show ipv6 tcp connect statistics	
Parameter Description	Parameter	Description
	local-ipv6 <i>X:X:X:X::X</i>	Local IPv6 address
	local-port <i>num</i>	Local port

	peer-ipv6 <i>X:X:X:X::X</i>	Peer IPv6 address																																																	
	peer-port <i>num</i>	Peer port																																																	
	statistics	Displays IPv6 TCP connection statistics																																																	
Defaults	N/A																																																		
Command Mode	Privileged EXEC mode																																																		
Usage Guide	N/A																																																		
Configuration Examples	The following example displays the current IPv6 TCP connection information. <pre>FS#show ipv6 tcp connect</pre> <table><thead><tr><th>Number</th><th>Local Address</th><th>Foreign Address</th><th>State</th><th>Process name</th></tr></thead><tbody><tr><td>1</td><td>:::22</td><td>:::0</td><td>LISTEN</td><td>sshd</td></tr><tr><td>2</td><td>:::23</td><td>:::0</td><td>LISTEN</td><td>telnetd</td></tr><tr><td>3</td><td>1000::1:23</td><td>1000::2:64201</td><td>ESTABLISHED</td><td>telnetd</td></tr></tbody></table> The following example displays the current IPv6 TCP connection statistics. <pre>FS#show ipv6 tcp connect statistics</pre> <table><thead><tr><th>State</th><th>Count</th></tr></thead><tbody><tr><td colspan="2">-----</td></tr><tr><td>ESTABLISHED</td><td>1</td></tr><tr><td>SYN_SENT</td><td>0</td></tr><tr><td>SYN_RECV</td><td>0</td></tr><tr><td>FIN_WAIT1</td><td>0</td></tr><tr><td>FIN_WAIT2</td><td>0</td></tr><tr><td>TIME_WAIT</td><td>0</td></tr><tr><td>CLOSED</td><td>0</td></tr><tr><td>CLOSE_WAIT</td><td>0</td></tr><tr><td>LAST_ACK</td><td>0</td></tr><tr><td>LISTEN</td><td>1</td></tr><tr><td>CLOSING</td><td>0</td></tr><tr><td>Total:</td><td>2</td></tr></tbody></table>			Number	Local Address	Foreign Address	State	Process name	1	:::22	:::0	LISTEN	sshd	2	:::23	:::0	LISTEN	telnetd	3	1000::1:23	1000::2:64201	ESTABLISHED	telnetd	State	Count	-----		ESTABLISHED	1	SYN_SENT	0	SYN_RECV	0	FIN_WAIT1	0	FIN_WAIT2	0	TIME_WAIT	0	CLOSED	0	CLOSE_WAIT	0	LAST_ACK	0	LISTEN	1	CLOSING	0	Total:	2
Number	Local Address	Foreign Address	State	Process name																																															
1	:::22	:::0	LISTEN	sshd																																															
2	:::23	:::0	LISTEN	telnetd																																															
3	1000::1:23	1000::2:64201	ESTABLISHED	telnetd																																															
State	Count																																																		

ESTABLISHED	1																																																		
SYN_SENT	0																																																		
SYN_RECV	0																																																		
FIN_WAIT1	0																																																		
FIN_WAIT2	0																																																		
TIME_WAIT	0																																																		
CLOSED	0																																																		
CLOSE_WAIT	0																																																		
LAST_ACK	0																																																		
LISTEN	1																																																		
CLOSING	0																																																		
Total:	2																																																		
Related Commands	Command	Description																																																	
	N/A	N/A																																																	
Platform Description	N/A																																																		

10.8 show ipv6 tcp pmtu

	Use this command to display information about IPv6 TCP PMTU.																				
	show ipv6 tcp pmtu [local-ipv6 X:X:X:X::X] [local-port num] [peer-ipv6 X:X:X:X::X] [peer-port num]																				
Parameter Description	Parameter	Description																			
	local-ipv6 X:X:X:X::X	Local IPv6 address																			
	local-port num	Local port																			
	peer-ipv6 X:X:X:X::X	Peer IPv6 address																			
	peer-port num	Peer port																			
Defaults	N/A																				
Command Mode	Privileged EXEC mode																				
Usage Guide	N/A																				
Configuration Examples	The following example information about IPv6 TCP PMTU. FS# show ipv6 tcp pmtu <table><tr><th>Number</th><th>Local Address</th><th>Foreign Address</th><th>PMTU</th></tr><tr><td>1</td><td>1000::1:23</td><td>1000::2.13560</td><td></td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Number</td><td>Number</td></tr><tr><td>Local Address</td><td>Local address and port number. The number after the last colon is the port number.</td></tr><tr><td>Foreign Address</td><td>Remote address and port number. The number after the last colon is the port number.</td></tr><tr><td>PMTU</td><td>Path MTU.</td></tr></table>			Number	Local Address	Foreign Address	PMTU	1	1000::1:23	1000::2.13560		Field	Description	Number	Number	Local Address	Local address and port number. The number after the last colon is the port number.	Foreign Address	Remote address and port number. The number after the last colon is the port number.	PMTU	Path MTU.
Number	Local Address	Foreign Address	PMTU																		
1	1000::1:23	1000::2.13560																			
Field	Description																				
Number	Number																				
Local Address	Local address and port number. The number after the last colon is the port number.																				
Foreign Address	Remote address and port number. The number after the last colon is the port number.																				
PMTU	Path MTU.																				
Related Commands	Command	Description																			
	N/A	N/A																			
Platform Description	N/A																				

10.9 show ipv6 tcp port

	Use this command to display the current IPv6 TCP port status.
	show ipv6 tcp port [num]

Parameter Description	Parameter	Description																										
	num	Port number																										
Defaults	N/A																											
Command Mode	Privileged EXEC mode																											
Usage Guide	N/A																											
Configuration Examples	The following example displays the current IPv6 TCP port status. FS#show ipv6 tcp port TCP connections on port 23: <table><tr><td>Number</td><td>Local Address</td><td>Foreign Address</td><td>State</td></tr><tr><td>1</td><td>1000::1:23</td><td>1000::2:64571</td><td>ESTABLISHED</td></tr></table> Total: 1 TCP connections on port 2650: <table><tr><td>Number</td><td>Local Address</td><td>Foreign Address</td><td>State</td></tr><tr><td colspan="4">Total: 0</td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Number</td><td>Number</td></tr><tr><td>Local Address</td><td>Local address and port number.</td></tr><tr><td>Foreign Address</td><td>Remote address and port number.</td></tr><tr><td>State</td><td> Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet. </td></tr></table>		Number	Local Address	Foreign Address	State	1	1000::1:23	1000::2:64571	ESTABLISHED	Number	Local Address	Foreign Address	State	Total: 0				Field	Description	Number	Number	Local Address	Local address and port number.	Foreign Address	Remote address and port number.	State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.
Number	Local Address	Foreign Address	State																									
1	1000::1:23	1000::2:64571	ESTABLISHED																									
Number	Local Address	Foreign Address	State																									
Total: 0																												
Field	Description																											
Number	Number																											
Local Address	Local address and port number.																											
Foreign Address	Remote address and port number.																											
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.																											

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.10 show tcp connect

	Use this command to display basic information about the current TCP connections.			
	show tcp connect [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]			
	Use this command to display the current IPv4 TCP connection statistics.			
	show tcp connect statistics			
Parameter Description	Parameter	Description		
	local-ip <i>a.b.c.d</i>	Local IP address.		
	local-port <i>num</i>	Local port.		
	peer-ip <i>a.b.c.d</i>	Peer IP address.		
	peer-port <i>num</i>	Peer port.		
	statistics	Displays IPv4 TCP connection statistics.		
Defaults	N/A			
Command Mode	Privileged EXEC mode			
Usage Guide	N/A			
Configuration Examples	The following example displays the current IPv4 TCP connection information.			
	FS#show tcp connect			
	Number	Local Address	Foreign Address	State Process name
	1	0.0.0.0:22	0.0.0.0:0	LISTEN sshd
	2	0.0.0.0:23	0.0.0.0:0	LISTEN telnetd
	3	1.1.1.1:23	1.1.1.2:64201	ESTABLISHED telnetd
	Field		Description	
	Number		Sequence number.	
	Local Address		The Local address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.	
	Foreign Address		The remote address and port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23" , "23" is the port number.	

	<table><tr><td>State</td><td>Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.</td></tr><tr><td>Process name</td><td>Process name.</td></tr></table>	State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.	Process name	Process name.
State	Current status of the TCP connection. There are eleven possible states: CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent out. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.				
Process name	Process name.				
	The following example displays the current IPv4 TCP connection statistics. <pre>FS#show tcp connect statistics State Count ----- ESTABLISHED 1 SYN_SENT 0 SYN_RECV 0 FIN_WAIT1 0 FIN_WAIT2 0 TIME_WAIT 0 CLOSED 0 CLOSE_WAIT 0 LAST_ACK 0 LISTEN 1 CLOSING 0 Total: 2</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				

Platform	N/A
Description	

10.11 show tcp parameter

	Use this command to show TCP parameters.	
	show tcp parameter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example shows TCP parameters. <pre>FS#show tcp parameter</pre> Hash table information: - Established hash bucket size: 16384 - Bind hash bucket size: 16384 Memory information: - Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages) - Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit: bytes) - Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes) - Current allocated memory: 0 - Current memory pressure flag: 0 SYN specific information: - Max SYN_RECV sockets per LISTEN socket: 65535 - Max SYN retries: 5 - Max SYN ACK retries: 5 Timewait specific information: - Max timewait sockets: 180000 - Current timewait sockets: 0 - Timewait recycle: 0 - Reuse timewait port: 0 Keepalive information: - Keepalive on: 0 - Idle period: 900 seconds - Interval: 75 seconds - Max probes: 6	

	MTU probing: Enable mtu probing: 0 FIN specific information: FIN_WAIT_2 timeout: 60 seconds Orphan socket information: Max orphans: 16384 Max orphan retries: 0 Current orphans: 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.12 show tcp pmtu

	Use this command to display information about TCP PMTU.		
	show tcp pmtu [local-ip <i>a.b.c.d</i>] [local-port <i>num</i>] [peer-ip <i>a.b.c.d</i>] [peer-port <i>num</i>]		
Parameter Description	Parameter	Description	
	local-ip <i>a.b.c.d</i>	Local IP address.	
	local-port <i>num</i>	Local port.	
	peer-ip <i>a.b.c.d</i>	Peer IP address.	
	peer-port <i>num</i>	Peer port.	
Defaults	N/A		
Command Mode	Privileged EXEC mode		
Usage Guide	N/A		
Configuration Examples	The following example displays PMTU of IPv4 TCP connection.		
	FS# show tcp pmtu		
	Number	Local Address	Foreign Address PMTU
	1	192.168.195.212.23	192.168.195.112.13560 1440
	Field	Description	
	Number	Sequence number.	
	Local Address	The local address and the port number. The number after the last “.” is the port number. For example, in “2002::2.23” and “192.168.195.212.23” ,	

		"23" is the port number.
	Foreign Address	The remote address and the port number. The number after the last "." is the port number. For example, in "2002::2.23" and "192.168.195.212.23", "23" is the port number.
	PMTU	PMTU value.
Related Commands	Command	Description
	ip tcp path-mtu-discovery	Enables the TCP PMTU discovery function.
Platform Description	N/A	

10.13 show tcp port

	Use this command to display information about the current TCP port.							
	show tcp port [<i>num</i>]							
Parameter Description	Parameter	Description						
	<i>num</i>	Port number						
Defaults	N/A							
Command Mode	Privileged EXEC mode							
Usage Guide	N/A							
Configuration Examples	The following example displays the current IPv4 TCP port status. <pre>FS#show tcp port TCP connections on port 23: Number Local Address Foreign Address State 1 1.1.1.1:23 1.1.1.2:64571 ESTABLISHED Total: 1 TCP connections on port 2650: Number Local Address Foreign Address State Total: 0</pre> Tcpv6 listen on 23 have total 1 connections. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Foreign Address</td><td>Remote address</td></tr><tr><td>State</td><td>Status of the current TCP connection. There are eleven possible states:</td></tr></table>		Field	Description	Foreign Address	Remote address	State	Status of the current TCP connection. There are eleven possible states:
Field	Description							
Foreign Address	Remote address							
State	Status of the current TCP connection. There are eleven possible states:							

	CLOSED: The connection has been closed. LISTEN: Listening state SYNSENT: In the three-way handshake phase when the SYN packet has been sent. SYNRCVD: In the three-way handshake phase when the SYN packet has been received. ESTABLISHED: The connection has been established. FINWAIT1: The local end has sent the FIN packet. FINWAIT2: The FIN packet sent by the local end has been acknowledged. CLOSEWAIT: The local end has received the FIN packet from the peer end. LASTACK: The local end has received the FIN packet from the peer end, and then sent its own FIN packet. CLOSING: The local end has sent the FIN packet from the peer end, and received the FIN packet from the peer end before the ACK packet for the peer end to respond with this FIN packet is received. TIMEWAIT: The FIN packet sent by the local end has been acknowledged, and the local end has also acknowledged the FIN packet.	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.14 show tcp statistics

	Use this command to show TCP statistics on received packets, three way handshake and time-wait.	
	show tcp parameter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example shows TCP parameters. <pre>FS#show tcp statistics TCP Packets</pre>	

	Received: 1103 Errors : 0(checksum: 0) Three way handshake Request queue overflow: 0 Accept backlog full: 0 Web authentication limit per user: 0 Failed to alloc memory for request sock: 0 Failed to create open request child: 0 SYN ACK retransmits: 0 Timeouted requests: 0 Time-wait Time-wait bucket table overflow: 0	
	Field Description	
	Field	Description
	TCP Packets	Normal packets and error packets
	Three way handshake	Three way handshake information, including session request count, server-client connection count, three way handshake failure count caused by Web authentication limit, TCP socket failure count caused by memory shortage, sub-session failure count, packet retransmission count and session failure count caused by retransmission timeout.
	Time-wait	Session in TIMEWAIT state
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11 IPv4/IPv6 REF Commands

11.1 clear ip ref packet statistics

	Use this command to clear IPv4 FS Express Forwarding (REF) packet statistics.	
	clear ip ref packet statistics	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears IPv4 REF packet statistics. <pre>FS #clear ip ref packet statistics</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.2 clear ipv6 ref packet statistics

	Use this command to clear IPv6 REF packet statistics.	
	clear ipv6 ref packet statistics	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears IPv6 REF packet statistics. <pre>FS #clear ipv6 ref packet statistics</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.3 ip ref load-sharing original

	Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv4 addresses. Use the no form of this command to restore the default setting.	
	ip ref load-sharing original	
	no ip ref load-sharing original	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default algorithm is based on the destination IPv4 address.	
Command Mode	Global configuration mode	
Usage Guide	The REF is responsible for data forwarding and supports two load balancing algorithms. One is based on destination IP addresses and the other is based on the source and destination IP addresses. When IP packets are forwarded on multiple paths, for example, when load balancing based on destination IP addresses is configured, the REF forwards packets based on a path matching the destination IP address of packets. By default, load balancing based on destination IP addresses is used.	
Configuration Examples	The following example configures the load balancing algorithm based on source and destination IP addresses. FS(config)# ip ref load-sharing original	
	The following example configures the load balancing algorithm based on destination IP addresses of packets. FS(config)# no ip ref load-sharing original	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.4 ip ref load-balance

	Use this command to configure ECMP load balancing algorithm. Use the no or default form of this command to restore the default setting.

	ip ref load-balance [src-dst-ip src-ip src-ip-src-dst-l4port src-dst-ip-src-dst-l4port]	
	no ip ref load-balance	
Parameter Description	Parameter	Description
	src-dst-ip	Configures ECMP load balancing based on the source and destination IP address. The packets containing the same source and destination IP address are routed over the same link. This algorithm is recommended for a layer-3 network scenario.
	src-ip	Configures ECMP load balancing based on the source IP address. The packets containing the same source IP address are routed over the same link.
	src-ip-src-dst-l4port	Configures ECMP load balancing based on the source IP address, layer-4 source port and layer-4 destination port. The packets containing the same the source IP address, layer-4 source port and layer-4 destination port are routed over the same link. The other packets are evenly distributed over ECMP paths.
	src-dst-ip-src-dst-l4port	Configures ECMP load balancing based on the source IP address, destination IP address, layer-4 source port and layer-4 destination port.
Defaults	ECMP load balancing is based on the source and the destination IP address by default.	
Command Mode	Global configuration mode	
Usage Guide		
Configuration Examples	The following example configures ECMP load balancing based on the destination IP address.	
	FS(config)# ip ref load-balance dst-ipe	
Configuration Examples	The following example restores the default ECMP load balancing algorithm.	
	FS(config)# no ip ref load-balance	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.5 ip ref hash-elasticity enable

	Use this command to enable ECMP elastic hash. Use the no or default form of this command to restore the default setting.
	ip ref hash-elasticity enable
	no ip ref hash-elasticity enable

Parameter Description	Parameter	Description
	N/A	N/A

Defaults ECMP elastic hash is disabled by default.

Command Mode Global configuration mode

Usage Guide N/A

Configuration The following example enables ECMP elastic hash.

Examples `ip ref hash-elasticity enable`

The following example disables ECMP elastic hash.

`no ip ref hash-elasticity enable`

Related Commands	Command	Description
	N/A	N/A

Platform N/A

Description

11.6 ipv6 ref load-sharing original

	Use this command to configure the algorithm that is used for load balancing during forwarding based on the source and destination IPv6 addresses. Use the no form of this command to restore the default setting.	
	ipv6 ref load-sharing original	
	no ipv6 ref load-sharing original	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default algorithm is based on the destination IPv6 address.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example restores the algorithm that is used for load balancing during forwarding to the default setting.	
	<code>FS(config)#no ipv6 ref load-sharing original</code>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A.	

11.7 show ip ref adjacency

	Use this command to display the information about the specified adjacent node or all adjacent nodes.	
	show ip ref adjacency [glean local <i>ip-address</i> interface <i>interface_type interface_number</i> discard statistics]	
Parameter Description	Parameter	Description
	glean	Aggregate adjacent node, which is used for a direct route
	local	Local adjacent node, which is used by the local host
	<i>ip-address</i>	Next-hop IP address
	<i>interface_type</i>	Interface type
	<i>interface_number</i>	Interface number
	discard	Displays discarded adjacent nodes.
	statistics	Statistics
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can be used to display the information about the adjacent node table in the current REF module. By specifying parameters, the information about the aggregate adjacent node, local adjacent node, adjacent node of the specified IP address, adjacent node associated with the specified interface, and all adjacent nodes can be displayed.	
Configuration Examples	The following example displays the information about all adjacent nodes in the adjacent node table. FS#show ip ref adjacency <pre> id state type rfct chg ip interface linklayer(header data) 1 unresolved mcast 1 0 224.0.0.0 9 resolved forward 1 0 192.168.50.78 GigabitEthernet 0/0 00 25 64 C5 9D 6A 00 D0 F8 98 76 54 08 00 7 resolved forward 1 0 192.168.50.200 GigabitEthernet 0/0 00 04 5F 87 69 66 00 D0 F8 98 76 54 08 00 6 unresolved glean 1 0 0.0.0.0 GigabitEthernet 0/0 4 unresolved local 3 0 0.0.0.0 Local 1 </pre> Description of fields:	

	Field	Description
	id	Adjacent node ID
	state	Adjacent node state: Unresolved Resolved
	type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency
	rfct	Reference count of the adjacent node
	chg	Whether the adjacent node is on the changing link.
	ip	IP address of the adjacent node
	interface	Interface
	linklayer	Layer 2 head
Related Commands	Command	Description
	show ip ref route	Displays all route information in the current REF module.
Platform Description	N/A	

11.8 show ip ref exact-route

	This command is used to display the IPv4 REF exact route.	
	show ip ref exact-route [oob vrf vrf_name] <i>source_ipaddress dest_ipaddress</i>	
Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf vrf_name	VRF name, supported only by the VRF-supported device.
	<i>source_ipaddress</i>	Source IP address of the packet
	<i>dest_ipaddress</i>	Destination IP address of the packet
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	This command is used to specify the source and the destination IP address of the IP packets, and to display the path of forwarding the current packet with REF																																			
Configuration	The following example displays the IPv4 REF exact route from 192.168.217.74 to 192.168.13.1.																																			
Examples	FS# show ip ref exact-route 192.168.217.74 192.168.13.1 192.168.217.74 --> 192.168.13.1 (vrf global): <table><tr><td>id</td><td>state</td><td>type</td><td>rfct</td><td>chg</td><td>ip</td><td>interface</td><td>linklayer(header data)</td></tr><tr><td>9</td><td>resolved</td><td>forward</td><td>1</td><td>0</td><td>192.168.17.1</td><td>GigabitEthernet 0/0</td><td>00 25 64 C5 9D 6A 00 D0 F8 98 76 54 08 00</td></tr></table> Description of fields: <table><tr><th>Field</th><th>Description</th></tr><tr><td>id</td><td>Adjacency ID</td></tr><tr><td>state</td><td>Adjacency state: Unresolved Resolved</td></tr><tr><td>type</td><td>Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency</td></tr><tr><td>rfct</td><td>Reference count of the adjacency</td></tr><tr><td>chg</td><td>Whether the adjacency is on the changing link.</td></tr><tr><td>ip</td><td>Adjacency IP address</td></tr><tr><td>interface</td><td>Interface</td></tr><tr><td>linklayer</td><td>Layer 2 head</td></tr></table>		id	state	type	rfct	chg	ip	interface	linklayer(header data)	9	resolved	forward	1	0	192.168.17.1	GigabitEthernet 0/0	00 25 64 C5 9D 6A 00 D0 F8 98 76 54 08 00	Field	Description	id	Adjacency ID	state	Adjacency state: Unresolved Resolved	type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency	rfct	Reference count of the adjacency	chg	Whether the adjacency is on the changing link.	ip	Adjacency IP address	interface	Interface	linklayer	Layer 2 head
id	state	type	rfct	chg	ip	interface	linklayer(header data)																													
9	resolved	forward	1	0	192.168.17.1	GigabitEthernet 0/0	00 25 64 C5 9D 6A 00 D0 F8 98 76 54 08 00																													
Field	Description																																			
id	Adjacency ID																																			
state	Adjacency state: Unresolved Resolved																																			
type	Adjacency type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency																																			
rfct	Reference count of the adjacency																																			
chg	Whether the adjacency is on the changing link.																																			
ip	Adjacency IP address																																			
interface	Interface																																			
linklayer	Layer 2 head																																			
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip ref route</td><td>Displays all routing information in the current REF module.</td></tr></table>	Command	Description	show ip ref route	Displays all routing information in the current REF module.																															
Command	Description																																			
show ip ref route	Displays all routing information in the current REF module.																																			
Platform Description	N/A																																			

11.9 show ip ref packet statistics

	Use this command to display IPv4 REF packet statistics.	
	show ip ref packet statistics	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	N/A																			
Command Mode	Privileged EXEC mode																			
Usage Guide	N/A																			
Configuration Examples	The following example displays IPv4 REF packet statistics. FS #show ip ref pkt-statistic ref packet statistic: bad head : 0 lookup fib fail : 0 local adj : 0 glean adj : 0 forward : 0 redirect : 0 punt adj : 0 outif not in ef : 0 ttl expiration : 0 no ip routing : 0 <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>total recved</td><td>Number of total packets received by REF</td></tr><tr><td>bad head</td><td>Number of the packets with false header</td></tr><tr><td>lookup fib fail</td><td>Number of the packets with failed REF routing</td></tr><tr><td>drop adj</td><td>Number of the packets matching the dropped adjacency</td></tr><tr><td>local adj</td><td>Number of the packets matching the local adjacency</td></tr><tr><td>glean adj</td><td>Number of the packets matching the gleaned adjacency</td></tr><tr><td>forward</td><td>Number of the packets matching the forwarded adjacency</td></tr><tr><td>no ip routing</td><td>Number of the packets not allowed to be forwarded and sent to local.</td></tr></tbody></table>		Field	Description	total recved	Number of total packets received by REF	bad head	Number of the packets with false header	lookup fib fail	Number of the packets with failed REF routing	drop adj	Number of the packets matching the dropped adjacency	local adj	Number of the packets matching the local adjacency	glean adj	Number of the packets matching the gleaned adjacency	forward	Number of the packets matching the forwarded adjacency	no ip routing	Number of the packets not allowed to be forwarded and sent to local.
Field	Description																			
total recved	Number of total packets received by REF																			
bad head	Number of the packets with false header																			
lookup fib fail	Number of the packets with failed REF routing																			
drop adj	Number of the packets matching the dropped adjacency																			
local adj	Number of the packets matching the local adjacency																			
glean adj	Number of the packets matching the gleaned adjacency																			
forward	Number of the packets matching the forwarded adjacency																			
no ip routing	Number of the packets not allowed to be forwarded and sent to local.																			
Related Commands	Command	Description																		
	N/A	N/A																		
Platform Description	N/A																			

11.10 show ip ref resolve-list

	Use this command to display the IPv4 REF resolution information.	
	show ip ref resolve-list	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays IPv4 REF resolution information.	
	FS#show ip ref resolve-list	
	IP res_state flags interface	
	1.1.1.1 unres 1 GigabitEthernet 0/0	
	Field	Description
	IP	IP address
	res_state	unres: unresolved res: resolved
flags	0: related to adjacency 1: unrelated to adjacency	
interface	Interface	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.11 show ip ref route

	Use this command to display all the routing information in the IPv4 REF table.	
	show ip ref route [oob vrf vrf_name] [default ip mask statistics]	
Parameter	Parameter	Description
Description		
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf vrf_name	VRF name, supported only by the VRF-supported device.
	default	Specifies the default route.
	ip	Specifies the destination IP address of the route
	mask	Specifies the mask of the route.

	statistics	Statistics																																																																				
Defaults	N/A																																																																					
Command Mode	Privileged EXEC mode																																																																					
Usage Guide	This command is used to display the related routing information on the current REF table, and specify the default route and all the routing information matching IP/MASK.																																																																					
Configuration Examples	The following example displays all the routing information in the IPv4 REF table. FS#show ip ref route Codes: * - default route # - zero route <table><tr><td>ip</td><td>mask</td><td>weight</td><td>path-id</td><td>next-hop</td><td>interface</td></tr><tr><td>255.255.255.255</td><td>255.255.255.255</td><td>1</td><td>4</td><td>0.0.0.0</td><td>Local 0</td></tr><tr><td>224.0.0.0</td><td>240.0.0.0</td><td>1</td><td>1</td><td>224.0.0.0</td><td></td></tr><tr><td>224.0.0.0</td><td>255.255.255.0</td><td>1</td><td>4</td><td>0.0.0.0</td><td>Local 0</td></tr><tr><td>192.168.50.0</td><td>255.255.255.0</td><td>1</td><td>6</td><td>0.0.0.0</td><td>FastEthernet 0/0</td></tr><tr><td>192.168.50.255</td><td>255.255.255.255</td><td>1</td><td>2</td><td>0.0.0.0</td><td></td></tr><tr><td>192.168.50.200</td><td>255.255.255.255</td><td>1</td><td>7</td><td>192.168.50.200</td><td>FastEthernet 0/0</td></tr><tr><td>192.168.50.122</td><td>255.255.255.255</td><td>1</td><td>4</td><td>0.0.0.0</td><td>Local 0</td></tr><tr><td>192.168.50.78</td><td>255.255.255.255</td><td>1</td><td>9</td><td>192.168.50.78</td><td>FastEthernet 0/0</td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>ip</td><td>Destination IP address</td></tr><tr><td>mask</td><td>Mask</td></tr><tr><td>path-id</td><td>Adjacent identity</td></tr><tr><td>next-hop</td><td>Address of next hop</td></tr><tr><td>weight</td><td>Routing weight</td></tr><tr><td>interface</td><td>Egress</td></tr></table>		ip	mask	weight	path-id	next-hop	interface	255.255.255.255	255.255.255.255	1	4	0.0.0.0	Local 0	224.0.0.0	240.0.0.0	1	1	224.0.0.0		224.0.0.0	255.255.255.0	1	4	0.0.0.0	Local 0	192.168.50.0	255.255.255.0	1	6	0.0.0.0	FastEthernet 0/0	192.168.50.255	255.255.255.255	1	2	0.0.0.0		192.168.50.200	255.255.255.255	1	7	192.168.50.200	FastEthernet 0/0	192.168.50.122	255.255.255.255	1	4	0.0.0.0	Local 0	192.168.50.78	255.255.255.255	1	9	192.168.50.78	FastEthernet 0/0	Field	Description	ip	Destination IP address	mask	Mask	path-id	Adjacent identity	next-hop	Address of next hop	weight	Routing weight	interface	Egress
ip	mask	weight	path-id	next-hop	interface																																																																	
255.255.255.255	255.255.255.255	1	4	0.0.0.0	Local 0																																																																	
224.0.0.0	240.0.0.0	1	1	224.0.0.0																																																																		
224.0.0.0	255.255.255.0	1	4	0.0.0.0	Local 0																																																																	
192.168.50.0	255.255.255.0	1	6	0.0.0.0	FastEthernet 0/0																																																																	
192.168.50.255	255.255.255.255	1	2	0.0.0.0																																																																		
192.168.50.200	255.255.255.255	1	7	192.168.50.200	FastEthernet 0/0																																																																	
192.168.50.122	255.255.255.255	1	4	0.0.0.0	Local 0																																																																	
192.168.50.78	255.255.255.255	1	9	192.168.50.78	FastEthernet 0/0																																																																	
Field	Description																																																																					
ip	Destination IP address																																																																					
mask	Mask																																																																					
path-id	Adjacent identity																																																																					
next-hop	Address of next hop																																																																					
weight	Routing weight																																																																					
interface	Egress																																																																					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip ref exact-route</td><td>Displays the accurate REF forwarding path of an IP packet.</td></tr></table>	Command	Description	show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.																																																																	
Command	Description																																																																					
show ip ref exact-route	Displays the accurate REF forwarding path of an IP packet.																																																																					
Platform Description	N/A																																																																					

11.12 show ipv6 ref adjacency

	Use this command to display the information about the IPv6 adjacent node.																																					
	show ipv6 ref adjacency [glean local <i>ipv6-address</i> interface <i>interface_type</i> <i>interface_number</i> discard statistics]																																					
Parameter Description	Parameter	Description																																				
	glean	Aggregate adjacent node, which is used for a direct route																																				
	local	Local adjacent node, which is used by the local host																																				
	<i>ipv6-address</i>	Next-hop IP address																																				
	<i>interface_type</i>	Interface type																																				
	<i>interface_number</i>	Interface number																																				
	discard	Displays discarded adjacent nodes.																																				
	statistics	Statistics																																				
Defaults	N/A																																					
Command Mode	Privileged EXEC mode																																					
Usage Guide	This command can be used to display the information about the adjacent node table in the privileged EXEC mode and global configuration mode.																																					
Configuration Examples	The following example displays the information about the IPv6 adjacent node.. <pre>FS#show ipv6 ref adjacency</pre> <table><tr><th>id</th><th>state</th><th>type</th><th>rfct</th><th>chg</th><th>ip</th><th>interface</th><th>linklayer(header data)</th></tr><tr><td>1</td><td>unresolved</td><td>glean</td><td>1</td><td>0</td><td>::</td><td>GigabitEthernet 0/0</td><td></td></tr><tr><td>2</td><td>unresolved</td><td>local</td><td>2</td><td>0</td><td>::1</td><td>Local 1</td><td></td></tr></table> Description of fields: <table><tr><th>Field</th><th>Description</th></tr><tr><td>id</td><td>Adjacent node ID</td></tr><tr><td>state</td><td>Adjacent node state: Unresolved Resolved</td></tr><tr><td>type</td><td>Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency</td></tr><tr><td>rfct</td><td>Reference count of the adjacent node</td></tr><tr><td>chg</td><td>Whether the adjacent node is on the changing link.</td></tr></table>		id	state	type	rfct	chg	ip	interface	linklayer(header data)	1	unresolved	glean	1	0	::	GigabitEthernet 0/0		2	unresolved	local	2	0	::1	Local 1		Field	Description	id	Adjacent node ID	state	Adjacent node state: Unresolved Resolved	type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency	rfct	Reference count of the adjacent node	chg	Whether the adjacent node is on the changing link.
id	state	type	rfct	chg	ip	interface	linklayer(header data)																															
1	unresolved	glean	1	0	::	GigabitEthernet 0/0																																
2	unresolved	local	2	0	::1	Local 1																																
Field	Description																																					
id	Adjacent node ID																																					
state	Adjacent node state: Unresolved Resolved																																					
type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency																																					
rfct	Reference count of the adjacent node																																					
chg	Whether the adjacent node is on the changing link.																																					

	ip	IP address of the adjacent node
	interface	Interface
	linklayer(header data)	Layer 2 head
For distributed routers, id is divided into two fields, namely, gid and lid, standing for global adjacent node ID and local adjacent node ID respectively.		
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.13 show ipv6 ref exact-route

	This command is used to display the IPv6 REF exact route.					
	show ipv6 ref exact-route [oob vrf vrf_name] <i>source-ipv6-address destination-ipv6-address</i>					
Parameter Description	Parameter	Description				
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.				
	vrf vrf_name	VRF name, supported only by the VRF-supported device.				
	source-ipv6-address	Source IP address of the packet				
	destination-ipv6-address	Destination IP address of the packet				
Defaults	N/A					
Command Mode	Privileged EXEC mode					
Usage Guide	N/A					
Configuration Examples	The following example displays the IPv4 REF exact route from 2001:db8:1::1 to 3001:db8:2::2.					
	FS#show ipv6 exact-route 2001:db8:1::1 3001:db8:2::2					
	2001:db8:1::1 --> 3001:db8:2::2 (vrf global):					
	ID	state type rfct chg ip interface linklayer(header data)				
	3	unresolve glean 1 0 :: GigabitEthernet 0/0				
	Description of fields:					
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>id</td><td>Adjacent node ID</td></tr></table>	Field	Description	id	Adjacent node ID	
Field	Description					
id	Adjacent node ID					

		state	Adjacent node state: Unresolved Resolved		
		type	Adjacent node type Local: local adjacency Forward: forward adjacency Discard: discard adjacency Glean: glean adjacency Mcast: multicast adjacency		
		rfct	Reference count of the adjacent node		
		chg	Whether the adjacent node is on the changing link.		
		ip	IP address of the adjacent node		
		interface	Interface		
		linklayer(header data)	Layer 2 head		
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

11.14 show ipv6 ref packet statistics

	Use this command to display IPv6 REF packet statistics.	
	show ipv6 ref packet statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays IPv6 REF packet statistics. <pre>FS#show ipv6 ref packet statistics ref packet statistic: bad head : 0</pre>	

	<pre>lookup fib fail : 0 local adj : 0 glean adj : 0 forward : 0 redirect : 0 hop-limit expiration : 0 no ipv6 unicast-routing : 0</pre>																	
	<table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>bad head</td><td>Number of the packets with false header</td></tr><tr><td>lookup fib fail</td><td>Number of the packets with failed REF routing</td></tr><tr><td>drop adj</td><td>Number of the packets matching the dropped adjacency</td></tr><tr><td>local adj</td><td>Number of the packets matching the local adjacency</td></tr><tr><td>glean adj</td><td>Number of the packets matching the gleaned adjacency</td></tr><tr><td>forward</td><td>Number of the packets matching the forwarded adjacency</td></tr><tr><td>no ip routing</td><td>Number of the packets not allowed to be forwarded and sent to local.</td></tr></tbody></table>	Field	Description	bad head	Number of the packets with false header	lookup fib fail	Number of the packets with failed REF routing	drop adj	Number of the packets matching the dropped adjacency	local adj	Number of the packets matching the local adjacency	glean adj	Number of the packets matching the gleaned adjacency	forward	Number of the packets matching the forwarded adjacency	no ip routing	Number of the packets not allowed to be forwarded and sent to local.	
Field	Description																	
bad head	Number of the packets with false header																	
lookup fib fail	Number of the packets with failed REF routing																	
drop adj	Number of the packets matching the dropped adjacency																	
local adj	Number of the packets matching the local adjacency																	
glean adj	Number of the packets matching the gleaned adjacency																	
forward	Number of the packets matching the forwarded adjacency																	
no ip routing	Number of the packets not allowed to be forwarded and sent to local.																	
Related Commands	Command	Description																
	N/A	N/A																
Platform Description	N/A																	

11.15 show ipv6 ref resolve-list

	This command is used to display the IPv6 REF resolution information.	
	show ipv6 ref resolve-list	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples	The following example displays IPv6 REF resolution information.	
	FS#show ipv6 ref resolve-list	
	<pre> IP res_state flags interface 1000::1 unres 1 GigabitEthernet 0/0 </pre>	
	Field	Description
	IP	IPv6 address
	res_state	unres: unresolved res: resolved
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.16 show ipv6 ref route

	Use this command to display all the routing information in the IPv6 REF table.	
	show ipv6 ref route [oob vrf vrf-name] [default statistics prefix/len]	
Parameter Description	Parameter	Description
	oob	Out of band, namely, the network that the management interface belongs to, supported only by the device supporting the management interface.
	vrf vrf_name	VRF name, supported only by the VRF-supported device.
	default	Specifies the default route.
	statistics	Statistics
	prefix/len	Displays the route with the specified prefix (X:X:X:X/<0-128>).
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display all routing information in the IPv6 REF table. If there is no VRF parameter, information about the global REF table is displayed; if there is VRF parameter, information about the specified VRF table is displayed. The command can also be used to display information about the default route, the route with the specified prefix, and statistics of all types of routes.	

Configuration Examples	The following example displays all the routing information in the REF IPv6 table.		
	FS#show ipv6 ref route		
	Codes: * - default route		
	prefix/len	weight	path_id next_hop interface
	2001:da8:ffe:2::/64	1	3 :: GigabitEthernet 0/0
	2001:da8:ffe:2::3/128	1	2 ::1 Local 1
	fe80::/10	1	6 :: Null 0
	fe80::21a:a9ff:fe3b:fa41/128	1	2 ::1 Local 1
	Field		Description
	prefix/len		IPv6 prefix and prefix length.
path-id		Adjacent identity	
next-hop		Address of next hop	
weight		Routing weight	
interface		Interface	
Related Commands	Command		Description
	N/A		N/A
Platform Description	N/A		

11.17 show ip ref load-balance

	Use this command to display ECMP load balancing configuration.	
	show ip ref load-balance	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration	The following example displays ECMP load balancing configuration..	

Examples	FS# FS#show ip ref load-balance load-balance : src-dst-ip. hash-elasticity : enable. FS#	
	Field	Description
	load-balance	ECMP load balancing algorithm
	hash-elasticity	Enable: Enable elastic hash. Disable: Disable elastic hash.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

Multicast Commands

1 IPv4 Multicast Routing Configuration Commands

1.1 clear ip mroute

	Use this command to remove the forwarding information of the IP multicast routes. clear ip mroute { * <i>group-address</i> [<i>source -address</i>] }	
Parameter Description	Parameter	Description
	*	Remove all the forwarding information in the IP multicast route table.
	<i>group-address</i>	Group IP address of IP multicast routes.
	<i>source-address</i>	Source IP address of multicast routess.
Command Mode	Privileged EXEC mode.	
Examples	The following example removes the entry whose group IP address is 230.0.0.1 from the multicast routing table: FS# clear ip mroute 230.0.0.1	
Related Commands	Command	Description
	show ip mroute	Show the forwarding information of multicast routes.

1.2 clear ip mroute statistics

	this command to remove the statistics of IP multicast routes. clear ip mroute statistics { * <i>group-address</i> [<i>source -address</i>] }	
Parameter Description	Parameter	Description
	*	Remove all the forwarding entries in the multicast route table.
	<i>group-address</i>	Group IP address of IP multicast routes
	<i>source-address</i>	Source IP address of multicast route.
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	

Examples	The following example clears the statistics of entry with the group IP address 230.0.0.1 from the multicast routing table.	
	FS# clear ip mroute statistics 230.0.0.1	
Related Commands		
	Command	Description
	show ip mroute	Show the multicast route forwarding information.
	clear ip mroute	Clear the multicast route forwarding information.

1.3 ip mroute

	Use this command to configure static multicast routes. Use the no or default form of this command to delete the configured routes.	
	ip mroute <i>source-address mask</i> { <i>[protocol]</i> { <i>rpf-address</i> <i>interface-type interface-number</i> } <i>[distance]</i> }	
	no ip mroute <i>source-address mask</i> <i>[protocol]</i>	
	default ip mroute <i>source-address mask</i> <i>[protocol]</i>	
Parameter Description	Parameter	Description
	source-address	Source IP address of the multicast route
	mask	Mask of the source IP address
	protocol	(Optional) The unicast routing protocol being used.
	rpf-address	Incoming interface of the multicast route
	interface-type interface-number	Interface type and interface ID.
	distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.
Default	<i>distance</i> : 0.	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command is used to configure the route for the purpose of RFF check. Note that the configured route is prior to the route learned in the unicast form.	
Examples	The following example allows the multicast routes of all the sources in a network to pass 172.30.10.13: <pre>FS(config)# ip mroute 172.16.0.0 255.255.0.0 172.30.10.13</pre>	

1.4 ip multicast-routing

	Use this command to enable multicast routing forwarding. The no form of this command disables multicast routing forwarding.	
	ip multicast-routing <i>[vrf vrf-name]</i>	
	no ip multicast-routing <i>[vrf vrf-name]</i>	
Parameter Description	Parameter	Description
	vrf vrf-name	Specify the VRF instance.
Default	Disabled.	

Command Mode	Privileged EXEC mode.
Usage Guide	This command allows you to enable IPv4 multicast routing forwarding. The multicast protocol will not be enabled with IPv4 multicast routing forwarding disabled.  It is not recommended to configure different v4 multicast routing protocols on different interfaces of a device.
Examples	This command enables multicast routing forwarding. <pre>FS(config)# ip multicast-routing</pre>

1.5 ip multicast-boundary

	Use this command to configure the boundary of an IP multicast group. Use the no or default form of this command to remove the configured boundary.	
	ip multicast boundary <i>access-list</i> [in out]	
	no ip multicast boundary <i>access-list</i> [in out]	
	default ip multicast boundary <i>access-list</i> [in out]	
Parameter	Parameter	Description
Description	<i>access-list</i>	Access list associated with the multicast boundary.
	in	Inbound direction.
	out	Outbound direction.
Default	The boundary of a specified IP multicast group is defined by default.	
Command Mode	Interface configuration mode	
Usage Guide	Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IP address. Note: This command filters IGMP and PIMSM packets of the specified IP address range. Multicast packets will not be received and sent through the interface of the boundary.	
Examples	The following example configures svi1 as the boundary of all IP multicast groups. <pre>FS(config)# ip access-list mul-boun FS(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255 FS(config-std-nacl)#exit FS(config)# interface vlan 1 FS(config-if)# ip multicast boundary mul-boun</pre>	

1.6 ip multicast route-limit

	Use this command to limit the number of the entries that can be added to the multicast routing table. Use the no or default form of this command to remove the configuration.	
	ip multicast route-limit <i>limit</i> [<i>threshold</i>]	
	no ip multicast route-limit <i>limit</i>	
	default ip multicast route-limit	
Parameter	Parameter	Description
Description	<i>limit</i>	The number of the entries that can be added to the multicast routing table is 1 to 2147483647. The default value is 1024.
	<i>threshold</i>	(Optional) Number of multicast routes at which alarms will be triggered. The default value is 2147483647.
Default	The default value of <i>limit</i> is 1024. The default value of <i>threshold</i> is 2147483647.	
Command Mode	Global configuration mode.	
Usage Guide	Note that the hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.	
Examples	The following example sets the route limit to 500.	
	FS(config)# ip multicast route-limit 500	

1.7 ip multicast longest-match

	Select the multicast static routing, MBGP routing and unicast routing that could be used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules. Use this command to select the one with the mask longest-matched from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing. Use the no or default form of this command restores it to the default setting. By default, select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.	
	ip multicast rpf longest-match	
	no ip multicast rpf longest-match	
	default ip multicast rpf longest-match	
Parameter	Parameter	Description
Description	N/A	N/A
Default	Use the RPF rule to select the optimal routing for RPF check from the multicast static routing, MBGP routing and	

	unicast routing that are used for the RPF check from the multicast static routing table, MBGP routing table and unicast routing table respectively by following the RPF rules. Then select one routing of the highest priority from the three routings. If the routings are in the same priority, select the routing in order of multicast static routing, MBGP routing, unicast routing.
Command Mode	Global configuration mode.
Examples	The following example configures to select the routing with the longest-match. FS(config)# ip multicast rpf longest-match

1.8 ip multicast static

	Use this command to enable flow control for multicast packets on the Layer 2 interface. Use the no or default form of this command removes the setting.	
	ip multicast static <i>source-address group-address interface-type interface-number</i>	
	no ip multicast static <i>source-address group-address interface-type interface-number</i>	
	default ip multicast static <i>source-address group-address interface-type interface-number</i>	
Parameter	Parameter	Description
Description	<i>source-address</i>	Source IP address
	<i>group-address</i>	IP address of the multicast group
	<i>interface-type</i> <i>interface number</i>	<i>Layer 2 interface on which multicast packets are allowed to forward</i>
Default	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces. This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-DM or PIM-SM) may be affected because some features of the multicast protocol are driven by multicast flows.	
Examples	The following example configures forwarding multicast flows (192.168.43.4 and 255.1.1.5) through GigabitEthernet 2/6 and FastEthernet 3/2. <pre>FS(config)# ip multicast static 192.168.43.4 225.1.1.5 G2/6 FS(config)# ip multicast static 192.168.43.4 225.1.1.5 F3/2</pre>	

1.9 ip multicast ttl-threshold

	Use this command to configure TTL (time-to-live) threshold on the interface. Use the no or default form of the command to restore it to the default value.

	ip multicast ttl-threshold <i>ttl-value</i>	
	ip multicast ttl-threshold	
	default ip multicast ttl-threshold	
Parameter	Parameter	Description
Description	<i>ttl-value</i>	TTL threshold on the interface, within the range of 0 to 255.
Default	The default <i>ttl-value</i> is 0.	
Command Mode	Interface configuration mode.	
Usage Guide	Use show running-config to display configuration. A device with multicast enabled can maintain one TTL threshold for every interface. If the TTL of the multicast packet received is greater than the threshold of the interface, the packets will be forwarded. Otherwise, the packet is discarded. Note that the TTL threshold is effective only to the multicast frames. In addition, you must configure it on the L3 interface.	
Examples	The following example sets the TTL threshold on the interface to 5. <pre>FS(config-if)# ip multicast ttl-threshold 5</pre>	

1.10 msf force-forwarding

	Use this command to enable IPv4 multicast data packets destined for the CPU to be forcedly forwarded by software. Use the no or default form of this command to restore the default settings.	
	msf force-forwarding	
	no msf force-forwarding	
	default msf force-forwarding	
Parameter	Parameter	Description
Description	N/A	N/A
Default	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Examples	The following example enable IPv4 multicast data packets destined for the CPU to be forcedly forwarded by software. <pre>FS(config)# msf force-forwarding</pre>	

1.11 msf ipmc-overflow override

	Use this command to enable the overflow overriding mechanism. Use the no or default form of this command to remove the configuration.	
	msf ipmc-overflow override	
	no msf ipmc-overflow override	
	default msf ipmc-overflow override	
Parameter	Parameter	Description
Description	-	-
Default	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Examples	The following example enables the overflow overriding mechanism. <pre>FS (config)# msf ipmc-overflow override FS (config)#</pre>	

1.12 msf nsf

	Use this command to configure the parameter for the continuous multicast forwarding. Use the no or default form of this command to remove the configuration.	
	msf nsf {{convergence-time time} {leak interval} }	
	no msf nsf {convergence-time leak}	
	default msf nsf {convergence-time leak}	
Parameter	Parameter	Description
Description	convergence-time <i>tvl-value</i>	Maximum time for the multicast protocol convergence, in the valid range of the 0-3600s.
	leak <i>interval</i>	Packet multicast leak time, in the valid range of 0-3600s
Default	convergence-time <i>time</i> :140s; leak interval: 150s	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Examples	The following example sets the maximum time for the protocol convergence.	

```
FS (config)# msf nsf convergence-time 300
FS (config)#
```

The following example sets the packets leak time:

```
FS(config)# msf nsf leak 200
FS(config)#
```

1.13 show ip mrf mfc

Use this command to show the IPv4 multicast routing forwarding table.

show ip mrf mfc [*source-address group-address*]

Parameter	Parameter	Description						
Description	source-address	Source address of the multicast routing forwarding entries.						
	group-address	Group address of the multicast routing forwarding entries.						
Default	-							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode							
Usage Guide	The three parameters in this command are optional, wherein the source address and group address must be specified at the same time. ● If no source address and group address are specified, all mfc entries are displayed. ● When the source address and group address are specified only, the entries corresponding to the source and group addresses are displayed.							
Examples	The following example shows all IPv4 layer-3 multicast routing forwarding entries with source address 20.0.1.30. <pre>FS#show ip mrf mfc 20.0.1.30 233.3.3.3</pre> Multicast Routing and Forwarding Cache Table (20.0.1.30, 233.3.3.3) FAST_SW, SWITCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0 Incoming interface: VLAN 1[4097] Outgoing interface list: VLAN 3 (1) The fields in the execution of the show ip mrf mfc command are described in the following table. <table><tr><th>Field</th><th>Description</th></tr><tr><td>20.0.1.30</td><td>Source address of the entry.</td></tr><tr><td>233.3.3.3</td><td>Group address of the entry.</td></tr></table>		Field	Description	20.0.1.30	Source address of the entry.	233.3.3.3	Group address of the entry.
Field	Description							
20.0.1.30	Source address of the entry.							
233.3.3.3	Group address of the entry.							

		FAST_SW	The Flag shows whether to allow the fast forwarding or not. If the non-Ethernet interface, ppp, hdlc and frame relay exist, no fast forwarding entry generates.
		SWTCHED	Indicate whether the entry configuration on the next layer forwarding table has done not not.
		MIN_MTU MTU	The minimum MTU of the entry.
		MIN_MTU_IFINDEX	The interface index with the minimum MTU value.
		WRONG IF	The statistics number of the multicast data packets received on the wrong incoming interface.
		Incoming interface	Incoming interface of the entry.
		VLAN 3 (1)	The layer-3 outgoing interface of the entry is VLAN3. 1 for the ttl threshold of this layer-3 interface.

1.14 show ip mroute

	Use this command to show the IPv4 multicast routing forwarding table. show ip mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [dense sparse] [summary count]	
Parameter	Parameter	Description
Description	group-or-source-address	Multicast or source IP address
	group-or-source-address	Multicast or source IP address. The two addresses must not be the multicast addresses or source addresses at the same time.
	dense	Show PIM-DM multicast routing table.
	sparse	Show PIM-SM multicast routing table.
	summary	Show the summary of the multicast routing table.
	count	Show the count of the multicast routing table.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	The three parameters in this command are optional, wherein the source address and group address must be specified at the same time. ● If no source address and group address are specified, all mfc entries are displayed. ● When the source address and group address are specified only, the mfc entries corresponding to the source and group addresses are displayed.	
Examples	The following example shows the information of the multicast routing table: <pre>FS# show ip mroute IP Multicast Routing Table Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed Timers: Uptime/Stat Expiry Interface State: Interface (TTL)</pre>	

```
(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
```

```
Owner PIM-SM, Flags: TF
```

```
Incoming interface: FastEthernet 2/1
```

```
Outgoing interface list:
```

```
FastEthernet 1/3
```

The following example shows the information of a specific entry:

```
FS# show ip mroute 10.10.1.52 224.0.1.3
```

```
IP Multicast Routing Table
```

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
```

```
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface (TTL)
```

```
(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
```

```
Owner PIM-SM, Flags: TF
```

```
Incoming interface: FastEthernet 2/1
```

```
Outgoing interface list:
```

```
FastEthernet 1/3
```

The following example shows the count of the routing table:

```
FS# show ip mroute count
```

```
IP Multicast Statistics
```

```
Total 1 routes using 132 bytes memory
```

```
Route limit/Route threshold: 2147483647/2147483647
```

```
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 1/0/0
```

```
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
```

```
Immediate/Timed stat updates sent to clients: 0/0
```

```
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
```

```
Next stats poll: 00:01:10
```

```
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
```

```
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
```

```
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
```

```
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent
```

```
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
```

```
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example shows the summary of the routing table:

```
FS# show ip mroute summary
```

```
IP Multicast Routing Table
```

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
```

```
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface (TTL)
```

```
(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: T
```

	Field	Description
	Flags	I-Immediate statistic T-Timed statistic F-Already set to the forwarding table
	Timers:Uptime/Stat Expiry	Time when the entry is created. Time when it is aged.
	Interface State	Interface state.
	Owner	Owner of the entry, which may be a multicast routing protocol
	Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
	Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
	Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
	Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.
Related Commands	Command	Description
	ip multicast-routing	Enabling the multicast routing forwarding.
	ip pim dense-mode	Enable the PIM-DM on the interface.
	ip pim sparse-mode	Enable the PIM-SM on the interface.

1.15 show ip mroute static

	Use this command to show the v4 static multicast routing information.	
	show ip mroute static	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuraion mode	
Usage Guide	In the same conditions, the priority of the static multicast routing is higher than the dynamically learned.	
Examples	The following example shows the information of the user-configured static multicast routing: <pre>FS#show ip mroute static Mroute: 172.16.0.0, RPF neighbor: 172.30.10.13 Protocol: , distance: 0</pre>	

1.16 show ip mvif

	Use this command to show the basic information of the multicast interface.	
	show ip mvif { <i>interface-type interface-number</i> }	
Parameter	Parameter	Description
Description	<i>interface-type interface-number</i>	Interface Type and number
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuraion mode	
Examples	The following example shows the basic information of the multicast interface of svil. <pre>FS#show ip mvif vlan 1 Interface Vif Owner TTL Local Remote Uptime Idx Module Address Address VLAN 1 1 PIM-DM 2 192.168.1.1 0.0.0.0 00:13:16</pre>	

1.17 show ip rpf

	Use this command to show the RPF information of the specified source IP address.	
	show ip rpf { <i>source-address</i> }	
Parameter	Parameter	Description
Description	<i>source-address</i>	Specified source IP address
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuraion mode	
Usage Guide	The three parameters in this command are optional, wherein the source address and group address must be specified at the same time. ● If no source address and group address are specified, all mfc entries are displayed. ● When the source address and group address are specified only, the mfc entries corresponding to the source and group addresses are displayed.	
Examples	The following example shows the information of the RPF to 192.168.1.54: <pre>FS# show ip rpf 192.168.1.54 RPF information for 192.168.1.54 RPF interface: VLAN 1 RPF neighbor: 0.0.0.0 RPF route: 192.168.1.0/24 RPF type: unicast (connected) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 0</pre>	

Metric: 0

1.18 show ip rpf

	Use this command to show IPv4 multi-layer multicast forwarding table.																							
	show msf msc [source-address] [group-address]																							
Parameter	Parameter	Description																						
Description	source-address	Specified source IP address of the multi-layer multicast forwarding table.																						
	group-address	Specified group address of the multi-layer multicast forwarding table.																						
Default	-																							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuraion mode																							
Usage Guide	The three parameters in this command are optional. ● If only the source address is specified as s1, all msc entries with source address 1 are displayed. ● If the source address is specified as s1 and the group address as g1, all corresponding msc entries are displayed. ● Each parameter shall be input in order. Only when the parameter in front has been configured, the following one could be set.																							
Examples	The following example shows the IPv4 layer-3 multicast forwarding entries with source IP address 192.168.195.25: <pre>FS# show msf msc 192.168.195.25</pre> Multicast Switching Cache Table (192.168.195.23, 233.3.3.3, 1), SYNC, MTU:0, 1 OIFs VLAN 1(0): 1 OPORTs, REQ: DONE OPORT 6, IGMP-SNP, REQ: DONE The fields in the execution of the show mrf mfc command are described in the following table. <table><tr><th>Field</th><th>Description</th></tr><tr><td>192.168.195.23</td><td>Source address of the entry.</td></tr><tr><td>233.3.3.3</td><td>Group address of the entry.</td></tr><tr><td>1</td><td>Vlan id where the incoming interface of the entry is.</td></tr><tr><td>SYNC</td><td>The entry has been synchronized to the hardware.</td></tr><tr><td>MTU</td><td>MTU value</td></tr><tr><td>OIFs</td><td>Layer-3 outgoing interface number.</td></tr><tr><td>VLAN1(0)</td><td>The vlan where the layer-3 outgoing interface oif is.</td></tr><tr><td>1 OPORTs</td><td>The number of layer-2 port in the layer-3 outgoing oif.</td></tr><tr><td>REQ: DONE</td><td>This oif configuration on the hardware has done.</td></tr><tr><td>OPORT 6</td><td>The layer-2 port in the oif with index 6.</td></tr></table>		Field	Description	192.168.195.23	Source address of the entry.	233.3.3.3	Group address of the entry.	1	Vlan id where the incoming interface of the entry is.	SYNC	The entry has been synchronized to the hardware.	MTU	MTU value	OIFs	Layer-3 outgoing interface number.	VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.	1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.	REQ: DONE	This oif configuration on the hardware has done.	OPORT 6	The layer-2 port in the oif with index 6.
Field	Description																							
192.168.195.23	Source address of the entry.																							
233.3.3.3	Group address of the entry.																							
1	Vlan id where the incoming interface of the entry is.																							
SYNC	The entry has been synchronized to the hardware.																							
MTU	MTU value																							
OIFs	Layer-3 outgoing interface number.																							
VLAN1(0)	The vlan where the layer-3 outgoing interface oif is.																							
1 OPORTs	The number of layer-2 port in the layer-3 outgoing oif.																							
REQ: DONE	This oif configuration on the hardware has done.																							
OPORT 6	The layer-2 port in the oif with index 6.																							

	IGMP-SNP	This port is created by the IGMP SNOOPING protocol. This value can also be the PIM-SNP, which means this port is created by the PIM SNOOPING protocol. And the ROUTER means this port is created by the layer-3 protocol.
	REQ: DONE	The port configuration on the hardware has done.

1.19 show msf nsf

	Use this command to show the configuration of continuous multicast forwarding.	
	show msf nsf	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuraion mode	
Examples	The following example shows the configuration of continuous multicast forwarding. <pre> FS# show msf nsf Multicast HA Parameters -----+-----+ protocol convergence timeout 120 secs flow leak interval 20 secs FS# </pre>	
Related Commands	Command	Description
	msf nsf	Configure the multicast NSF parameter.

2 IPv6 Multicast Routing Commands

2.1 clear ipv6 mroute

	Use this command to remove the specific or all IPv6 multicast forwarding entries.	
	clear ipv6 mroute { * <i>v6group-address</i> [<i>v6source -address</i>]}	
Parameter	Parameter	Description
Description	*	Removes all the forwarding information in the IPv6 multicast route table.
	<i>v6group-address</i>	Group IPv6 address of IPv6 multicast routes
	<i>v6source-address</i>	Source IPv6 address of multicast routes
Command Mode	Privileged EXEC mode	
Configuration Examples	The following example removes all the multicast routing entries. FS# clear ip mroute *	
Related Commands	Command	Description
	show ipv6 mroute	N/A
	clear ipv6 mroute statistics	N/A

2.2 clear ipv6 statistics

	Use this command to remove the statistics of IPv6 multicast routes.	
	clear ipv6 mroute statistics { * <i>v6group-address</i> [<i>v6source -address</i>]}	
Parameter	Parameter	Description
Description	*	Removes all the forwarding entries in the multicast route table.
	<i>v6group-address</i>	Group IPv6 address of IPv6 multicast routes
	<i>v6source-address</i>	Source IPv6 address of multicast route
Command Mode	Privileged EXEC mode	
Usage Guide	-	
Configuration Examples	The following example clears all the statistical information of the multicast routing entries. FS# clear ip mroute statistics *	
Related Commands	Command	Description
	show ipv6 mroute	Displays the multicast route forwarding information.
	clear ipv6 mroute	Clears the multicast route forwarding information.

2.3 ipv6 mroute

	Use this command to configure static IPv6 multicast routes. Use the no or default form of this command to restore the default setting.	
	ipv6 mroute <i>ipv6-prefix/prefix-length</i> [<i>protocol</i>] { <i>v6rpf-address</i> <i>interface-type interface-number</i> } [<i>distance</i>]	
	no ipv6 mroute <i>ipv6-prefix/prefix-length</i> [<i>protocol</i>]	
	default ipv6 mroute <i>ipv6-prefix/prefix-length</i> [<i>protocol</i>]	
Parameter Description	Parameter	Description
	ipv6-prefix/prefix-length	Source IPv6 address of the multicast route
	mask	Mask of the source IPv6 address
	protocol	(Optional) The unicast routing protocol being used
	v6rpf-address	Incoming interface of the multicast route
	interface-type interface-number	Interface type and interface ID
	distance	Management distance used to determine whether to use the route for RPF routing, ranging from 1 to 255. The default value is 0.
Defaults	The static IPv6 multicast routing is not configured by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure the route for the purpose of RPF check. Note that the configured route is prior to the route learned in the unicast form. If the outgoing direction of static multicast route but not the next-hop IP shall be specified, the outgoing direction must be of the point-to-point type.	
Configuration Examples	The following example allows the static multicast route 2233::/64 to pass 3333::3333: <pre>FS(config)# ipv6 mroute 2233::/64 3333::3333</pre>	

2.4 ipv6 multicast boundary

	Use this command to configure the boundary of an IPv6 multicast group. Use the no form of this command to restore the default setting.	
	ipv6 multicast boundary <i>access-list-name</i> [in out]	
	no ipv6 multicast boundary <i>access-list-name</i> [in out]	
Parameter Description	Parameter	Description
	access-list-name	Access list associated with the multicast boundary
	in	Inbound redirection
	out	Outbound direction
Defaults	The boundary of a specified IPv6 multicast group is not defined by default.	
Command Mode	Interface configuration mode	

Usage Guide	Note that the ACL associated with the multicast boundary is either standard ACL or extended ACL. But the extended ACL only match the destination IPv6 address.  This command filters MLD, PIM-SMv6 packets of the specified IPv6 address range. Multicast packets will not be received and sent through the interface of the boundary.
Configuration Examples	The following example configures svi1 as the boundary of all IPv6 multicast groups. <pre>FS(config)# ip access-list mul-boun FS(config-std-nacl)# permit ip 233.3.3.0 0.0.0.255 FS(config-std-nacl)#exit FS(config)# interface vlan 1 FS(config-if)# ip multicast boundary mul-boun</pre>

2.5 ipv6 multicast route-limit

	Use this command to limit the number of the entries that can be added to the IPv6 multicast routing table. Use the no or global form of this command to restore the default setting.	
	ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	
	no ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	
	default ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	
Parameter Description	Parameter	Description
	<i>limit</i>	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 2147483647
	<i>threshold</i>	(Optional) Number of IPv6 multicast routes at which alarms will be triggered
Defaults	The default value of <i>limit</i> is 1024. The default value of <i>threshold</i> is 2147483647.	
Command Mode	Global configuration mode	
Usage Guide	The hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.	
Configuration Examples	The following example sets the route limit to 500 and the warning value 90. <pre>FS(config)# ipv6 multicast route-limit 500 90</pre>	

2.6 ipv6 multicast rpf longest-match

	Use this command to limit the number of the entries that can be added to the IPv6 multicast routing table. Use the no or global form of this command to restore the default setting.	
	ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	
	no ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	

	default ipv6 multicast route-limit <i>limit</i> [<i>threshold</i>]	
Parameter Description	Parameter	Description
	<i>limit</i>	The number of the entries that can be added to the IPv6 multicast routing table is 1 to 2147483647
	<i>threshold</i>	(Optional) Number of IPv6 multicast routes at which alarms will be triggered
Defaults	The default value of <i>limit</i> is 1024. The default value of <i>threshold</i> is 2147483647.	
Command Mode	Global configuration mode	
Usage Guide	The hardware resources of different devices are limited. The routes exceeding the hardware resource will be forwarded by software, which leads to lower product performance.	
Configuration Examples	The following example sets the route limit to 500 and the warning value 90. <pre>FS(config)# ipv6 multicast route-limit 500 90</pre>	

2.7 ipv6 multicast static

	Use this command to enable flow control for multicast packets on the Layer 2 interface. Use the no or default form of this command to restore the default setting.	
	ipv6 multicast static <i>source-address group-address interface-type interface-number</i>	
	no ipv6 multicast static <i>source-address group-address interface-type interface-number</i>	
	default ipv6 multicast static <i>source-address group-address interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>source-address</i>	Source IPv6 address
	<i>group-address</i>	IPv6 address of the multicast group
	<i>interface-type</i> <i>interface number</i>	2-layer interface on which multicast packets are allowed to forward
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	You can configure more than one command (or more than one interface) for a multicast flow. With flow control enabled, the multicast flow can only be forwarded through these configured interfaces. This command controls the forwarding of multicast flows on an interface without any direct influence on the packet processing of multicast protocols. However, the action of a multicast protocol (for instance, PIM-SMv6) may be affected because some features of the multicast protocol are driven by multicast flows.	

Configuration Examples	The following example configures forwarding multicast flows (2222::3333, ff66::100) through GigabitEthernet 2/6 and FastEthernet 3/2. <pre>FS(config)# ipv6 multicast static 2222::3333 ff66::100 G2/6 FS(config)# ipv6 multicast static 2222::3333 ff66::100 F3/2</pre>

2.8 ipv6 multicast-routing

	Use this command to enable the IPv6 multicast routing forwarding. Use the no or default form of this command to restore the default setting.	
	ipv6 multicast-routing	
	no ipv6 multicast-routing	
	default ipv6 multicast-routing	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable the IPv6 multicast routing forwarding. With this function disabled, the multicast protocol cannot be enabled.  This command must be configured to enable the IPv6 multicast routing forwarding. This function conflicts with IGMP Snooping.	
Configuration Examples	The following example enables the IPv6 multicast routing forwarding. <pre>FS(config)# ipv6 multicast-routing</pre> The following example disables the IPv6 multicast routing forwarding. <pre>FS(config)#no ipv6 multicast-routing</pre>	

2.9 msf6 force-forwarding

	Use this command to enable IPv6 multicast data packets destined for the CPU to be forcedly forwarded by software. Use the no or default form of this command to restore the default settings.	
	msf6 force-forwarding	
	no msf6 force-forwarding	
	default msf6 force-forwarding	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Global configuration mode
Usage Guide	N/A
Examples	The following example enable IPv6 multicast data packets destined for the CPU to be forcedly forwarded by software. <pre>FS(config)# msf6 force-forwarding</pre>

2.10 msf6 nsf

	Use this command to configure parameters for multicast non-stop forwarding. Use the no or default form of this command to restore the default setting.	
	msf6 nsf { convergence-time time leak interval }	
	no msf6 nsf { convergence-time leak }	
	default msf6 nsf {convergence-time leak}	
Parameter Description	Parameter	Description
	convergence-time time	Maximum duration for which the system waits for multicast protocol convergence The unit is second. The value ranges from 0 to 3600.
	leak interval	Interval at which multicast packets are leaked The unit is second. The value ranges from 0 to 3600.
Defaults	The default convergence-time is 20 seconds and leak interval is 30 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the maximum duration for which the system waits for multicast protocol convergence. <pre>FS (config)# msf6 nsf convergence-time 300</pre> The following example sets the interval at which multicast packets are leaked. <pre>FS(config)# msf6 nsf leak 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.11 show ipv6 mrf6 mfc

	Use this command to display the IPv6 multicast forwarding table.	
	show ipv6 mrf6 mfc [<i>v6source-address v6group-address</i>]	
Parameter	Parameter	Description
Description	<i>v6group-address</i>	IPv6 address of a multicast group
	<i>v6source-address</i>	IPv6 address of a multicast source
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	The two parameters are optional. The source address and group address must be specified together. If the two parameters are not specified, all mrf table entries will be displayed. If the two parameters are specified, the mrf entries of the specified source address and group address are displayed.	
Configuration Examples	The following example displays the 3-layer multicast forwarding table entries of IPv6 (the source address is 2000::1 and the group address is FF55::1). <pre> FS#show ipv6 mrf6 mfc 2000::1 FF55::1 Multicast Routing and Forwarding Cache6 Table (2000::1, FF55::1) FAST_SW, SWITCHED, MIN_MTU: 1500, MIN_MTU_IFINDEX: 4099, WRONG IF: 0 Incoming interface: VLAN 1[4097] Outgoing interface list: VLAN 3 (1) </pre>	
	Field	Description
	2000::1	Source address of entries
	FF55::1	Group address of entries
	FAST_SW	Indicates whether the entries allow fast forwarding, that is, whether the entries can be forwarded by using hardware or software forwarding. If the entries include an interface that does not support the multicast function (for example, the GRE tunnel interface), fast forwarding is not allowed.
	SWITCHED	Indicates whether the entries have been placed in the forwarding table on the next layer.
	MIN_MTU MTU	Minimum MTU value of entries
	MIN_MTU_IFINDEX	Index of the interface that has the minimum MTU value
	WRONG IF	Number of multicast packets sent from the wrong inbound interface
	VLAN 1[4097]	Indicates that the rpf inbound interface is VLAN1. 4097 indicates the IFINDEX of the interface.
	VLAN 3 (1)	Indicates that the 3-layer outbound interface of the entries is VLAN 3. 1 indicates the ttl threshold of the 3-layer interface.

Related		
Commands	N/A	N/A
Platform	N/A	
Description		

2.12 show ipv6 mroute

	Use this command to display the IPv6 multicast forwarding table. show ipv6 mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [sparse] [summary count]	
Parameter Description	Parameter	Description
	group-or-source-address	Multicat group IPv6 address
	group-or-source-address	Multicast source IPv6 address
	sparse	Displays the core entry of the multicast routing table.
	summary	Displays the summary of the multicast routing table.
	count	Displays the count of the multicast routing table.
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	

Configuration Examples

The following example displays all information of the IPv6 multicast routing table.

```
FS# show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SMv6, Flags: TF
Incoming interface: FastEthernet 2/1
Outgoing interface list:
FastEthernet 1/3
```

The following example displays the count of the routing table.

```
FS# show ipv6 mroute count
IPv6 Multicast Statistics
Total 1 routes using 168 bytes memory
Route limit/Route threshold: 1024/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 77/147/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 77/147/0
Immediate/Timed stat updates sent to clients: 0/29
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:09
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent
(2222::1234, ff56::1234), Forwarding: 1/0, Other: 0
Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following example displays the summary of the routing table.

```
FS# show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(2222::1234, ff56::1234), 00:00:28/00:03:25, PIM-SMv6, Flags: TF
```

Field	Description
Flags	I-Immediate statistic
	T-Timed statistic
	F-Already set to the forwarding table
Timers:Uptime/Stat Expiry	Time when the entry is created.
	Time when it is aged.
Interface State	Interface state.

	Owner	Owner of the entry, which may be a multicast routing protocol
	Incoming interface	Expected packet incoming interface. If the actual incoming interface does not match it, the packets will be discarded.
	Outgoing interface list	Outgoing interface list; the packets will be forwarded on the interfaces in the list.
	Forwarding Counts: Pkt count/Byte count,	Forwarding count: packet count/byte count forwarded by the entry
	Other Counts: Wrong If pkts	Count of the packets received from the wrong incoming interface.

Related Commands	Command	Description
	clear ipv6 mroute	N/A
	clear ipv6 mroute statistics	N/A

2.13 show ipv6 mroute static

	Use this command to display the static IPv6 multicast routing information. show ipv6 mroute static

Parameter	Parameter	Description
Description	N/A	N/A

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode

Usage Guide	

Configuration Examples	The following example displays the static IPv6 multicast routing information.
	<pre>FS#show ipv6 mroute static Mroute: 2233::/64, RPF neighbor: 3333::3333 Protocol: , distance: 0</pre>

2.14 show ipv6 mvif

	Use this command to display the basic information of the multicast interface. show ipv6 mvif { interface-type interface-number }

Parameter	Parameter	Description
Description	<i>interface-type interface-number</i>	Interface type and number

Command	
Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode

Configuration Examples	The following example displays the basic information of the multicast interface of svil. <pre>FS#show ipv6 mvif Interface Mif Owner Uptime Idx Module Register 0 03d03h09m VLAN 1 1 PIMSMV6 03d03h09m</pre>

2.15 show ipv6 rpf

	Use this command to display the RPF information of the specified source IPv6 address. show ipv6 rpf <i>v6source-address</i>

Parameter	Parameter	Description
Description	<i>v6source-address</i>	Specified source IPv6 address

Command	
Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode

Configuration Examples	The following example displays the information of the RPF to 2222::3333: <pre>FS# show ipv6 rpf 2222::3333 RPF interface: GigabitEthernet 0/1 RPF neighbor: :: RPF route: 2222::/64 RPF type: unicast (connected) RPF recursion count: 0 Doing distance-preferred lookups across tables Distance: 0 Metric: 0</pre>

2.16 show msf6 msc

	Use this command to display entries of the IPv6 routing multicast data stream exchange table.	
	show msf6 msc [<i>v6source-address</i>] [<i>v6group-address</i>] [<i>vlan-id</i>]	
Parameter	Parameter	Description
Description	<i>v6group-address</i>	IPv6 address of a multicast group
	<i>v6source-address</i>	IPv6 address of a multicast source

	<i>vlan-id</i>	VLAN ID of the inbound interface of the entries If the value is greater than 4096, the interface is a routing interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	This command is used to display entries of the IPv6 routing multicast data stream exchange table. The three parameters are all optional. If only the source address is specified and set to s1, msc entries of this source address will be displayed. If the source address is set to s1 and the group address is set to g1, msc entries of this source address and group address will be displayed. If the source address is set to s1, the group address is set to g1, and the VLAN ID is set to v1, then msc entries that meet these three conditions will be displayed. You must specify these three parameters in sequence. That is, you must specify the current parameter before specifying the next.	
Configuration Examples	The following example displays entries of the IPv6 routing multicast data exchange table of source address 2000::1: <pre>FS# show msf6 msc 2000::1 Multicast Switching Cache Table (2000::1, FF55::1, 1), SYNC, MTU:0, 1 OIFs VLAN 4094(8190): 1 OPORTs, REQ: DONE OPORT 6, MLD-SNP, REQ: DONE</pre>	
	Field	Description
	2000::1	Source address of entries
	FF55::1	Group address of entries
	1	VLAN ID of the inbound interface of the entries
	SYNC	Indicates that the entries have been synchronized to the bottom-layer hardware.
	MTU	MTU value of the entries
	OIFs	Number of 3-layer interfaces of the entries
	VLAN 4094(8190)	Indicates a 3-layer outbound interface VLAN xxx (yyy). If the 3-layer interface is an SVI interface, the value of xxx is the VLAN VID of the SVI, and the value of yyy is the VLAN vid+4096. If the 3-layer interface is a routing interface, the value of xxx is the IFINDEX of the interface+4096, and the value of yyy is the IFINDEX. This facilitates the index management of all 3-layer interfaces.
	1 OPORTs	Number of 2-layer interfaces owned by this 3-layer exit oif
	REQ: DONE	Indicates that the oif has been set to the bottom-layer hardware. The value may be: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.
	OPORT 6	Indicates that the oif has a 2-layer interface with the interface number of 6.
	MLD-SNP	Indicates that the interface is created based on MLD SNOOPING. Alternatively, the value may be one of the following options:

		ROUTER: Indicates that the interface is created based on the 3-layer protocol. INHERIT_FM_MLD_SNP: Indicates that the interface is created based on the MLD SNOOPING protocol inherited from other entries.
	REQ: DONE	Indicates that the interface has been set to the bottom-layer hardware. The value may be: ADD: Waiting to be added. Usually it is waiting for a data stream to be triggered. DEL: Being deleted. DONE: Synchronized to the hardware.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.17 show msf6 nsf

	Use this command to display the multicast non-stop forwarding configuration.	
	show msf6 nsf	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the multicast non-stop forwarding configuration. <pre> FS# show msf6 nsf Multicast HA Parameters -----+-----+ protocol convergence timeout 120 secs flow leak interval 20 secs </pre>	
Related Commands	Command	Description
	msf6 nsf	Multicast non-stop forwarding
Platform Description	N/A	

3 IGMP Commands

3.1 clear ip igmp group

	Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.	
	clear ip igmp group [<i>group-address</i> [<i>interface-type interface-number</i>]]	
Parameter Description	Parameter	Description
	<i>group-address</i>	32-bit multicast group IP address
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	The IGMP buffer includes a list that contains the multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the entries from the IGMP buffer, use the clear ip igmp group command without parameters.	
Configuration Examples	The following example clears all group entries. FS# clear ip igmp group	
Related Commands	Command	Description
	show ip igmp groups	N/A
	show ip igmp interface	N/A
Platform Description	N/A	

3.2 clear ip igmp interface

	Use this command to clear the IGMP entry for the interface.	
	clear ip igmp interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number

Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	This command is used to clear the information on the interface that is generated when IGMP is configured. The information includes the number of report/leave packets, and group members on interfaces.				
Configuration Examples	The following example clears the IGMP entry for the interface. FS# clear ip igmp interface gi 0/1				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

3.3 ip igmp access-group

	Use this command to control a multicast group on the interface. Use the no or default form of this command to restore the default setting.	
	ip igmp access-group <i>access-list</i>	
	no ip igmp access-group	
	default ip igmp access-group	
Parameter Description	Parameter	Description
	<i>access-list</i>	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.
Defaults	This command is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	You can add several multicast groups into the specific interfaces of the host in a subnet. These multicast groups can be controlled using ip igmp access-group.  With the IGMPv3 enabled, when the multicast group accesses the control command, the extended ACL is associated. If the IGMP report information received is (S1, S2, S3...Sn, G), the corresponding ACL will be used by this command to the (0, G) for the matching check. In order to use this command normally, the (0, G) must be configured explicitly for the extended ACL so as to implement the normal filtering of (S1, S2,	

	S3...Sn, G).	
Configuration Examples	The following example adds the interface Ethernet 0/1 to the group 225.2.2.2. <pre>FS# configure terminal FS(config)# access-list 1 permit 225.2.2.2 0.0.0.0 FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp access-group 1</pre> The following example associates the group control list with the extended ACL on the interface Eth 0/1 which only processes the igmp protocol packets with source address 1.1.1.1 and group address 233.3.3.3. <pre>FS# configure terminal FS(config)# ip access-list extended ext_acl FS(config-ext-nacl)# permit ip host 1.1.1.1 host 233.3.3.3 FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp access-group ext_acl</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.4 ip igmp enforce-router-alert

	Use this command to receive IGMP packets with router-alert option , and discard those without the option.	
	ip igmp enforce-router-alert	
	Use the no form of this command to receive all IGMP packets.	
	no ip igmp enforce-router-alert	
	Use the default form of this command to restore the default setting.	
	default ip igmp enforce-router-alert	
Parameter Description	Parameter	Description
	-	-
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuration	The following example receives IGMP packets with router-alert option.
Examples	<pre>FS# configure terminal FS(config)#ip igmp enforce-router-alert</pre>
Platform	N/A
Description	

3.5 ip igmp enforce-source-subnet

	Use this command to receive only the IGMP report packet containing the source address in the same network segment as the port.	
	ip igmp enforce-source-subnet	
	Use the no form of this command to restore the default setting.	
	no ip igmp enforce-source-subnet	
	Use the default form of this command to restore the default setting.	
	default ip igmp enforce-source-subnet	
Parameter Description	Parameter	Description
	-	-
Defaults	The source IP address is not checked by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example receives only the IGMP report packet containing the source address in the same network segment as the port. <pre>FS# configure terminal FS(config)# ip igmp enforce-source-subnet</pre>	
Platform Description	N/A	

3.6 ip igmp immediate-leave group-list

	In the IGMPversion2 and IGMPversion3 versions, use this command to shorten the delay of leaving a group. This command is used when a single receiving host is connected to a single interface. Use the no or default form of this command to restore the default setting.
	ip igmp immediate-leave group-list <i>access-list</i>

	no ip igmp immediate-leave	
	default ip igmp immediate-leave	
Parameter Description	Parameter	Description
	access-list	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	If this command is not configured, the device will send a particular group query message upon receiving the leaving message from the interface. When the host response is timeout, the device stops forwarding packets to this interface. The length of timeout depends on the query interval of the last member and IGMP robustness variable. The default value is 2s. If this command is configured, the device does not send a particular group query message upon receiving the leaving message from the interface. Instead, it directly removes this interface from the IGMP buffer and notifies the IGMP protocol. This will shorten the time significantly.	
Configuration Examples	The following example provides the immediate leaving function for some multicast groups. Certainly, you must make sure each interface of these multicast groups have one group member only. <pre> FS# configure terminal FS(config)# access-list 1 permit 225.192.20.0 0.0.0.255 FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp immediate-leave group-list 1 FS(config-if-Ethernet 0/1)# exit </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.7 ip igmp join-group

	Use this command to configure the interface of the switch with host activities and adds it to a multicast group, so that the sub-switch can learn the corresponding group information. You can use this command to add an interface to a group. Use the no or default form of this command to restore the default setting.
	ip igmp join-group <i>group-address</i>

	no ip igmp join-group <i>group-address</i>	
	default ip igmp join-group <i>group-address</i>	
Parameter Description	Parameter	Description
	group-address	Multicast group IP address
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command enables the host activities for the IGMP interface. When the host function is enabled, the interface can initiate the report message and respond to the query message. If the IGMP function is enabled on the interface, the interface can initiate the report message, so that the interface can learn the configured group members. You can use this command to add an interface to a group.	
Configuration Examples	The following example adds a host group member manually. <pre>FS# configure terminal FS(config)# interface fast 0/1 FS(config-if-Ethernet 0/1)# ip igmp join-group 233.3.3.3 FS(config-if-Ethernet 0/1)# exit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 ip igmp last-member-query-count

	Use this command to configure the value of last-member-query-count. Use the no or default form of this command to restore the default setting.	
	ip igmp last-member-query-count <i>number</i>	
	no ip igmp last-member-query-count	
	default ip igmp last-member-query-count	
Parameter Description	Parameter	Description
	number	Value of the last member query count in the range from 2 to 7.
Defaults	The default is 2.	

Command Mode	Interface configuration mode				
Usage Guide	This command only supports IGMPv2 and IGMPv3. When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying last-member-query-count time. The device will delete information about this group member if no group member report is received within the waiting time. The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time				
Configuration Examples	The following example sets the value of last member query count to 3. <pre>FS# configure terminal FS(config)# interface ethernet 0 FS(config-if-Ethernet 0/1)# ip igmp last-member-query-count 3</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

3.9 ip igmp last-member-query-interval

	Use this command to set the time interval of sending the group query message. Use the no or default form of this command to restore the default setting.	
	ip igmp last-member-query-interval <i>interval</i>	
	no ip igmp last-member-query-interval	
	default ip igmp last-member-query-interval	
Parameter Description	Parameter	Description
	<i>interval</i>	The interval sending the group query message in the range from 1 to 255 in the unit of 0.1 second.
Defaults	The default is 10 (1 second).	
Command Mode	Interface configuration mode	
Usage Guide	This command only supports IGMPv2 and IGMPv3. When the interface of the device receives an IGMPv2 group leaving message, the device waits for duration of query interval multiplying last-member-query-count time. The device will delete information about this group member if no group member report is received within the waiting time.	

	The waiting time = last-member-query-interval * last-member-query-count + 1/2 * query-max-response-time	
Configuration Examples	The following example sets the interval of sending the group query message to 20 seconds. <pre>FS# configure terminal FS(config)# interface eth 0 FS(config-if-Ethernet 0/1)# ip igmp last-member-query-interval 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.10 ip igmp limit

	Use this command to globally set the maximum number of IGMP group records. Use the no or default form of this command to restore the default setting.	
	ip igmp limit <i>number</i> [except <i>access-list</i>] no ip igmp limit default ip igmp limit	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of IGMP states, depending on devices
	<i>except access-list</i>	Name of access control list in the range from 1 to 199, 1,300 to 2,699, or characters.
Defaults	Global: 65,536 Interface: 1,0124	
Command Mode	Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to configure the maximum number of IGMP group records globally or on interfaces. The messages of the members exceeding the threshold will not be saved in the IGMP buffer and will not be forwarded. The messages of the members will be ignored if they exceed the interface or global configuration. If the configured value in global configuration mode is less than that in interface configuration mode, take the former.	
Configuration Examples	The following example sets the maximum number to 400 globally and to 300 on interfaces except ACL 1. <pre>FS# configure terminal FS(config)# ip igmp limit 400 except acl1 FS(config)# interface eth 0/1</pre>	

	FS(config-if-Ethernet 0/1)# ip igmp limit 300 except acl1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.11 ip igmp mroute-proxy

	Use this command to configure an interface as an mroute-proxy interface that can transmit messages to its uplink ports. Use the no or default form of this command to restore the default setting.	
	ip igmp mroute-proxy <i>interface-type interface-number</i>	
	no ip igmp mroute-proxy	
	default ip igmp mroute-proxy	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Name of the relevant uplink interface
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use the ip igmp proxy-service command to set the uplink interface as the proxy-service interface. Use the ip igmp mroute-proxy command to set the downlink interface as the mroute-proxy interface. IGMP query packets are forwarded from the proxy-service interface to the mroute-proxy interface. IGMP report packets are forward reversely.	
Configuration Examples	The following example configures E0/1 as proxy-service E0/2 as mroute-proxy. <pre>FS(config)# interface eth 0/1 FS(config-if-Ethernet 0/1)# ip igmp proxy-service FS(config-if-Ethernet 0/1)# exit FS(config)# interface eth 0/2 FS(config-if-Ethernet 0/2)# ip igmp mroute-proxy</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.12 ip igmp proxy-service

	Use this command to enable the service function of all downlink mroute-proxy ports. If you run this command on an interface, the interface becomes the uplink port of the corresponding mroute-proxy that associates its downlink ports and maintains the group information reported by the downlink ports. Use the no or default form of this command to restore the default setting.	
	ip igmp proxy-service	
	no ip igmp proxy-service	
	default ip igmp proxy-service	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	Use the ip igmp proxy-service command to set the uplink interface as the proxy-service interface. Use the ip igmp mroute-proxy command to set the downlink interface as the mroute-proxy interface. The command can configure at most 32 proxy-service ports. The number of interface with IGMP Proxy enabled is limited by the supported multicast interface number. When receiving a query message, the proxy-service port responds according to the IGMP group member information maintained by the port itself. The member information maintained by the proxy-service port is collected from the interface configured with mroute-proxy. Therefore, if a port is configured with proxy-service, the port performs the host activities, but not the device activities. If switch port operation is performed on an interface with proxy-service command configured, the ip igmp mroute-proxy interface command configured on the associated downlink ports is automatically deleted.	
Configuration Examples	The following example configures E0/1 as proxy-service and E0/2 as mroute-proxy. <pre> FS(config)# interface eth 0/1 FS(config-if-Ethernet 0/1)# ip igmp proxy-service FS(config-if-Ethernet 0/1)# exit FS(config)# interface eth 0/2 FS(config-if-Ethernet 0/2)# ip igmp mroute-proxy </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.13 ip igmp query-interval

	Use this command to configure the query interval of an ordinary member. Use the no or default form of this command to restore the default setting.	
	ip igmp query-interval <i>seconds</i>	
	no ip igmp query-interval	
	default ip igmp query-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Query interval of ordinary member, in the range is from 1 to 18,000 in the unit of seconds.
Defaults	The default is 125 seconds.	
Command Mode	Interface configuration mode	
Usage Guide		
Configuration Examples	The following example configures the query interval of ordinary member to 120 seconds on the interface Ethernet 0. FS(config-if)# ip igmp query-interval 120	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.14 ip igmp query-max-response-time

	Use this command to configure the maximum response interval. Use the no or default form of this command to restore the default setting.	
	ip igmp query-max-response-time <i>seconds</i>	
	no ip igmp query-max-response-time	
	default ip igmp query-max-response-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	The maximum response interval, in the range from 1 to 25 seconds
Defaults	The default is 10 seconds.	

Command Mode	Interface configuration mode	
Usage Guide	This command controls the interval for the respondent to respond the query message before the device deletes the group information.	
Configuration Examples	The following example configures the maximum response interval to 20 seconds on the interface Ethernet 0. <pre>FS(config-if-Ethernet 0/1)# ip igmp query-max-response-time 20</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.15 ip igmp query-timeout

	Use this command to configure the time the device waits before it takes over as the querier. Use the no or default form of this command to restore the default setting.	
	ip igmp query-timeout <i>seconds</i>	
	no ip igmp query-timeout default ip igmp query-timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Time the device waits before it takes over as the querier, in the range from 60 to 300 in the unit of seconds.
Defaults	The default is 255 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	This device becomes the querier if no query packet is received in this duration.	
Configuration Examples	The following example configures the time the device waits before it takes over as the querier to 200 s seconds on the interface Ethernet 0/1. <pre>FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp query-timeout 200</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.16 ip igmp robustness-variable

	Use this command to change the value of the robustness variable. Use the no or default form of this command to restore the default setting.	
	ip igmp robustness-variable <i>number</i>	
	no ip igmp robustness-variable	
	default ip igmp robustness-variable	
Parameter Description	Parameter	Description
	<i>number</i>	The value of robustness variable, in the range from 2 to 7
Defaults	The default is 2.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the value of robustness variable to 3. <pre>FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp robustness-variable 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.17 ip igmp send-router-alert

	Use this command to send IGMP report packets with the Router Alert option. Use the no or default form of this command to restore the default setting.	
	ip igmp send-router-alert	
	no ip igmp send -router-alert	
	default ip igmp send -router-alert	

Parameter Description	Parameter	Description
	-	-
Defaults	The Router Alert option is not carried in IGMP packets by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sends IGMP report packets with the Router Alert option. <pre>FS# configure terminal FS(config)# ip igmp send-router-alert</pre>	
Platform Description	N/A	

3.18 ip igmp ssm-map enable

	Use this command to enable the igmp ssm-map function in the global configuration mode. Use the no form of this command to restore the default setting.	
	ip igmp ssm-map enable	
	no ip igmp ssm-map enable	
	default ip igmp ssm-map enable	
Parameter Description	Parameter	Description
	-	-
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	If this command is configured, the dynamically learned group information is added forcibly to the associated source record. This command is usually used together with the ip igmp ssm-map static command.	
Configuration Examples	The following example enables the igmp ssm-map function in the global configuration mode. <pre>FS(config)# ip igmp ssm-map enable FS(config)# ip igmp ssm-map static 11 192.168.2.2.</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.19 ip igmp ssm-map static

	Use this command to map the static ssm-map source IP address to the group records. Use the no or default form of this command to restore the default setting.	
	ip igmp ssm-map static <i>access-list source-address</i>	
	no ip igmp ssm-map static <i>access-list source-address</i>	
	default ip igmp ssm-map enable <i>access-list source-address</i>	
Parameter Description	Parameter	Description
	access-list	ACL name in the range 1 to 99, 1,300 to 1,999 or characters.
	source-address	Unicast address mapped to the group record.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used together with the ip igmp ssm-map enable and ip igmp ssm-map static command. After configuration, the port maps the corresponding source IP address to all received messages below v3 .	
Configuration Examples	The following example maps the source address 192.168.2.2 to all group records permitted by ACL 11. <pre>FS(config)# ip igmp ssm-map enable FS(config)# ip igmp ssm-map static 11 192.168.2.2.</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.20 ip igmp static-group

	Use this command to directly add an interface to a group. Use the no or default form of this command to restore the default setting.

	ip igmp static-group <i>group-address</i>	
	no ip igmp static-group <i>group-address</i>	
	default ip igmp static-group <i>group-address</i>	
Parameter Description	Parameter	Description
	<i>group-address</i>	Multicast group IP address
Defaults	The switch is not added to a multicast group by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command directly adds an interface to a multicast group. The difference from join-group is that it directly adds an interface to the group without interacting with a report message. You can use this command to add an interface to a group. The added interfaces by this command can only be deleted by using the no ip igmp static-group command.	
Configuration Examples	The following example adds a host group member. <pre>FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp static-group 236.6.6.6</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.21 ip igmp version

	Use this command to set the version number of IGMP to be used on the interface. Use the no or default form of this command to restore the default setting.	
	ip igmp version { 1 2 3 }	
	no ip igmp version	
	default ip igmp version	
Parameter Description	Parameter	Description
	1	IGMP v1
	2	IGMP v2
	3	IGMP v3

Defaults	The default is IGMPv2.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to globally configure the IGMP version. It should be noted that IGMP will reset after configuration.	
Configuration Examples	The following example sets the version number to 3. <pre>FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ip igmp version 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.22 show ip igmp groups

	Use this command to display the groups directly connected to the device and the group information learnt from IGMP.	
	show ip igmp groups [<i>interface-type interface-number</i>] [<i>group-address</i>] [detail]	
Parameter Description	Parameter	Description
	group-address	32-bit multicast group IP address, namely Category D address. 8 bits are in one group in decimal form. Groups are separated with dots.
	interface-type	Interface type
	interface-number	Interface number
	detail	Displays the detailed information
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command without any parameters to display group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if a group address is added to the command.	
Configuration	The following example displays information about all the groups.	

Examples	<pre>FS# show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 224.0.1.1 eth2 00:00:09 00:04:17 10.10.0.82 224.0.1.24 eth2 00:00:06 00:04:14 10.10.0.84 224.0.1.40 eth2 00:00:09 00:04:15 10.10.0.91 224.0.1.60 eth2 00:00:05 00:04:15 10.10.0.7 239.255.255.250 eth2 00:00:12 00:04:15 10.10.0.228 239.255.255.254 eth2 00:00:08 00:04:13 10.10.0.84</pre> The following example displays detailed information about a specific group. <pre>FS# show ip igmp groups 224.1.1.1 detail Interface : eth1 Group: 224.1.1.1 Uptime: 00:00:42 Group mode: Include Last reporter: 192.168.50.111 TIB-A Count: 2 TIB-B Count: 0 Group source list: (R - Remote, M - SSM Mapping) Source Address Uptime v3 Exp Fwd Flags 192.168.55.55 00:00:42 00:03:38 Yes R 192.168.55.66 00:00:42 00:03:38 Yes R</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.23 show ip igmp interface

	Use this command to display the information of this interface.	
	show ip igmp interface [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	Run this command without any parameter, and all interface information is displayed by default.	
Configuration	The following example displays the information of all the interfaces.	
Examples	FS# show ip igmp interface Interface vlan 1(Index 4294967295) IGMP Active, Non-Querier, Version 3 (default) IGMP querying router is 0.0.0.0 IGMP query interval is 125 seconds IGMP querier timeout is 255 seconds IGMP max query response time is 10 seconds Last member query response interval is 1000 milliseconds Group Membership interval is 260 seconds	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.24 show ip igmp ssm-mapping

		Use this command to display the ssm-map information of the IGMP configuration.
		show ip igmp ssm-mapping [<i>group-address</i>]
Parameter Description	Parameter	Description
	<i>group-address</i>	Source address to be mapped
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Run this command without any parameter, and all SSM-MAP information is displayed.	
Configuration Examples	The following example displays the ssm-map configuration information. <pre> FS#show ip igmp ssm-mapping 233.3.3.3 Group address: 233.3.3.3 Database : Static Source list : 192.3.3.3 : 3.3.3.3 </pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4 MLD Commands

4.1 clear ipv6 mld group

	Use this command to clear the dynamic group member learned by MLD protocol.	
	clear ipv6 mld group [<i>group-address</i>] [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>group-address</i>	IPv6 multicast group address with 128 bits
	<i>interface-type</i>	The associated interface type
	<i>interface-number</i>	The associated interface number
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	MLD maintains a list of the multicast groups to be added to the host in the directly-connected sub-net. Use the clear ipv6 mld group command to remove all dynamic group member record from the MLD group member list.	
Configuration Examples	The following example clears all group records. <pre>FS# clear ipv6 mld group</pre> The following example clears one group record. <pre>FS# clear ipv6 mld group ff1e::100</pre> The following example s clears the record on a specified interface. <pre>FS# clear ipv6 mld group ff1e::100 interfa fa0/1</pre>	
Related Commands	Command	Description
	show ipv6 mld groups	N/A
	show ipv6 mld interface	N/A
Platform Description	N/A	

4.2 clear ipv6 mld interface

	Use this command to clear all MLD statistical information and the group member records on the interface.
	clear ipv6 mld interface <i>interface-type interface-number</i>

Parameter Description	Parameter	Description
	<i>interface-type</i>	The interface type
	<i>interface-number</i>	The interface ID
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear all group information and some packet statistical information learned by LDP on the interface. Those packet statistical information include the number of the received report packets, the number of the done packets and the the number of the group members on the interface.	
Configuration Examples	The following example clears all MLD statistical information and the group member records on the interface. FS# clear ipv6 mld interface fa 1/1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.3 ipv6 mld access-group

	Use this command to filter the specific requested group on the interface. Only the report packets in accordance with the corresponding ACL are allowed to be processed. Use the no or default form of this command to restore the default setting.	
	ipv6 mld access-group <i>access-list</i>	
	no ipv6 mld access-group	
	default ipv6 mld access-group	
Parameter Description	Parameter	Description
	<i>access-list</i>	The IPv6 ACL name
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to filter some groups on the interface and associate with the corresponding ACLs. The correspondent ACL deny report packets will be discarded. This command supports the extended ACL and the	

	source record information of the MLDv2 packets can be filtered.  The multicast group access control command is associated with the extended ACL. When the received MLD report message is (S1,S2,S3...Sn,G), use this command to match and check the (0,G) message using the corresponding ACL. To this end, a (0,G) must be configured for the extended ACL to filter the (S1,S2,S3...Sn,G).					
Configuration Examples	The following example enables the group information carried in the report packets to be in accordance with acl for the normal handling on the interface Eth0/1. <pre>FS(config)#ipv6 access-list acl FS(config-ipv6-acl)#permit ipv6 ::/64 ff66::100/64 FS(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64 FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld access-group acl</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

4.4 ipv6 mld immediate-leave group-list

	Use this command to set the immediate-leave mechanism. With this command configured, the group within the range of group-list, will not send the query packet for the specific group and will remove this group from the group member list immediately after receiving the corresponding done packets. This function is used in the condition that there is only one multicast source that receives the host request on an interface. Use the no or default form of this command to restore the default setting.	
	ipv6 mld immediate-leave group-list <i>access-list</i>	
	no ipv6 mld immediate-leave group-list	
	default ipv6 mld immediate-leave group-list	
Parameter Description	Parameter	Description
	<i>access-list</i>	The IPv6 ACL name
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Without this command configured, when the device receives the MLD leave packets, the request packets for the specific groups will be sent. If there is still no host reply within the response time, the device will remove the	

	corresponding group record from the group member list. The timeout interval is determined by the last member query interval and the MLD robustness variable, and the default value is 2 seconds. With this command configured, when the device receives the MLD leave packets, it will not send the request packets for the specific groups, but remove the group information immediately, which reduces the leave delay greatly in the condition that there is only one host connecting to the interface.					
Configuration Examples	The following example configures the immediate-leave function. <pre>FS# configure terminal FS(config)#ipv6 access-list acl FS(config-ipv6-acl)#permit ipv6 2222::3333/64 ff66::100/64 FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld immediate-leave group-list acl</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

4.5 ipv6 mld join-group

	Use this command to configure the host action for the switch interface and add the related multicast group to the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 mld join-group <i>group-address</i>	
	no ipv6 mld join-group <i>group-address</i>	
	default ipv6 mld join-group <i>group-address</i>	
Parameter Description	Parameter	Description
	<i>group-address</i>	The IPv6 non-management multicast group address, which cannot start with 0xFF*1, 0xFF*2, and 0xFF3*
Defaults	The interface is not added to any group by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to enable the MLD host action on the interface. The interface can not only send the packets initiatively, but also reply to the query packets. Use this command if it is necessary to join a group member to the interface.	
Configuration	The following example adds the host group member:	

Examples	FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1-Ethernet 0/1)# ipv6 mld join-group ff55::100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.6 ipv6 mld last-member-query-count

	Use this command to set the last-member-query-count number. Use the no or default form of this command to restore the default setting.	
	ipv6 mld last-member-query-count <i>number</i>	
	no ipv6 mld last-member-query-count	
	default ipv6 mld last-member-query-count	
Parameter Description	Parameter	Description
	<i>number</i>	The last member query count number. The valid range is 2 to 7.
Defaults	The default is 2.	
Command Mode	Interface configuration mode	
Usage Guide	With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group (multiplied by the value of mld last-member-query-count) plus half the reply time.	
Configuration Examples	The following example sets the last-member-query-count number to 3. FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld last-member-query-count 3	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.7 ipv6 mld last-member-query-interval

	Use this command to set the time interval of sending the query packets to the specific group. Use the no or default form of this command to restore the default setting.	
	ipv6 mld last-member-query-interval <i>interval</i>	
	no ipv6 mld last-member-query-interval	
	default ipv6 mld last-member-query-interval	
Parameter Description	Parameter	Description
	<i>interval</i>	The valid range is 1-255 in the unit of 0.1 seconds.
Defaults	The default is 10 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	With the MLD leave packets received on the interface, if there is no group reply within the timeout interval, this group will be removed from the MLD group member list on the interface. The timeout interval is the query interval for the specific group(multiplied by the value of mld last-member-query-count) plus half the reply time.	
Configuration Examples	The following example sets the mld last-member-query-interval to 2 seconds. <pre> FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld last-member-query-interval 20 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.8 ipv6 mld limit

	Use this command to enable to learn the max-number of the group member through the MLD protocol. Use the no or default form of this command to restore the default setting.	
	ipv6 mld limit <i>number</i> [except <i>access-list</i>]	
	no ipv6 mld limit <i>number</i> [except <i>access-list</i>]	
	default ipv6 mld limit <i>number</i> [except <i>access-list</i>]	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum number of the group member learned by the MLD

	except <i>access-list</i>	(Optional) The ACL beyond the configured mld limit
Defaults	Interface: 1,024 Global: 65,536	
Command Mode	Interface configuration mode/Global configuration mode	
Usage Guide	Use this command to set the max-number of the group members learned through the MLD in the global configuration mode. If the group member number has exceeded the limit, the received report packets later will be discarded and fail to form the group record. If the except list has also been set at the same time, the group member packets, including the packets in the access-list, will be free from the member number limit. This command can also be used in the interface configuration mode. The configurations in two different configuration modes are independent. If the number limit in the global configuration mode is lower than the one in the interface configuration mode, the former configuration takes precedence.	
Configuration Examples	The following example sets the MLD limit to 400, but the configured ACL can still learn. <pre>FS(config-if)# ipv6 mld limit 300 except acl FS# configure terminal FS(config)# ipv6 mld limit 400 except acl1 FS(config)# interface eth 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld limit 300 except acl1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.9 ipv6 mld mroute-proxy

	Use this command to enable the interface to forward the packets to the correspondent connected interface. Use the no or default form of this command to restore the default setting.	
	ipv6 mld mroute-proxy <i>interface-type interface-number</i>	
	no ipv6 mld mroute-proxy	
	default ipv6 mld mroute-proxy	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	The correspondent connected interface
Defaults	This function is disabled by default.	

Command Mode	Interface configuration mode	
Usage Guide	Use the ipv6 mld proxy-service command to configure the uplink interface as proxy-service one. Use the ipv6 mld mroute-proxy command to configure the downlink interface as mroute-proxy one. After the connected interface has been configured as the proxy-service interface, it can forward the MLD packets sent from other members.	
Configuration Examples	The following example sets the interface as the mroute-proxy interface and enables multicast proxy. <pre>FS(config)# interface eth 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld proxy-service FS(config-if-Ethernet 0/1)# exit FS(config)# interface eth 0/2 FS(config-if-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.10 ipv6 mld proxy-service

	Use this command to enable the proxy-service function for the interface connected with the mroute-proxy interface in the downward direction. After configuring this command, the interface becomes the one connected with the mroute-proxy in the upward direction, and associates with and maintains the group information from the interfaces in the downward direction. Use the no or default form of this command to disable the default setting.	
	ipv6 mld proxy-service	
	no ipv6 mld proxy-service	
	default ipv6 mld proxy-service	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	Use the ipv6 mld proxy-service command to configure the uplink interface as proxy-service one.	

	Use the ipv6 mld mroute-proxy command to configure the downlink interface as mroute-proxy one. The configurable max-number limit is 32. The number of the interfaces with MLD Proxy enabled is limited by the number multicast interfaces supported device. After receiving the query packet, the proxy-service interface replies according to the member information, which are collected from the mroute-proxy interface and maintained by the proxy-service interface itself. With proxy-service configured, this interface owns the host action rather than the router action. The ipv6 mld mroute-proxy interface command configuration on the associated interface in the downward direction is removed automatically if the switchport operation is performed on the interfaces.	
Configuration Examples	The following example sets the interface proxy-service and enables multicast proxy. <pre>FS(config)# interface eth 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld proxy-service FS(config-if-Ethernet 0/1)# exit FS(config)# interface eth 0/2 FS(config-if-Ethernet 0/1-Ethernet 0/2)# ipv6 mld mroute-proxy eth 0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.11 ipv6 mld querier-timeout

	Use this command to set the querier alive period. Use the no or default form of this command to restore the default setting.	
	ipv6 mld querier-timeout <i>seconds</i>	
	no ipv6 mld querier-timeout	
	default ipv6 mld querier-timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	The querier alive period, in the range from 60 to 300 in the unit of seconds.
Defaults	The default is 255 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	After the querier sends the query packet, the querier will wait to receive the query packet sent by another querier within the alive period. If no packet is received by the first querier within the alive period, then the first querier takes itself as the only querier on the network segment.	

Configuration Examples	The following example sets the querier alive period to 200 seconds. <pre>FS(config-if-Ethernet 0/1)# ipv6 mld querier-timeout 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.12 ipv6 mld query-interval

	Use this command to set the query interval for the general member. Use the no or default form of this command to restore the default setting.	
	ipv6 mld query-interval <i>seconds</i>	
	no ipv6 mld query-interval	
	default ipv6 mld query-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	The query interval for the general member, in the range from 1 to 18,000 in the unit of seconds.
Defaults	The default is 125 seconds.	
Command Mode	Interface configuration mode	
Usage Guide		
Configuration Examples	The following example sets the query-interval for the general member on the interface Ethernet 0/1. <pre>FS(config-if-Ethernet 0/1)# ipv6 mld query-interval 120</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.13 ipv6 mld query-max-response-time

	Use this command to set the maximum response time. Use the no or default form of this command to restore the default setting.

	ipv6 mld query-max-response-time <i>seconds</i>	
	no ipv6 mld query-max-response-time	
	default ipv6 mld query-max-response-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	The maximum response time, in the range from 1 to 25 in the unit of seconds
Defaults	The default is 10 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to control the maximum response time of the host after the device sends the query packets. If there is no response within the maximum response time, MLD will remove the corresponding group from the group member list.	
Configuration Examples	The following example sets the maximum query response time on the interface Ethernet 0/1. <pre>FS(config-if-Ethernet 0/1)# ipv6 mld query-max-response-time 20</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.14 ipv6 mld robustness-variable

	Use this command to set querier robustness value.	
	Use the no or default form of this command to restore the default setting.	
	ipv6 mld robustness-variable <i>number</i>	
	no ipv6 mld robustness-variable	
	default ipv6 mld robustness-variable	
Parameter Description	Parameter	Description
	<i>number</i>	Sets the querier robustness value, in the range from 2 to 7.
Defaults	The default is 2.	
Command Mode	Interface configuration mode	

Usage Guide	N/A	
Configuration Examples	The following example sets the querier robustness value to 3. <pre>FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld robustness-variable 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.15 ipv6 mld ssm-map enable

	Use this command to enable the mld ssm-map function. Use the no or default form of this command to restore the default setting.	
	ipv6 mld ssm-map enable	
	no ipv6 mld ssm-map enable	
	default ipv6 mld ssm-map enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured, the group information dynamically learned will be added to the related source record forcibly. Usually, this command is set with the ipv6 mld ssm-map static command.	
Configuration Examples	The following example enables the mld ssm-map function in the global configuration mode. <pre>FS(config)# ipv6 mld ssm-map enable FS(config)# ipv6 mld ssm-map static 11 4444::1234</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.16 ipv6 mld ssm-map static

	Use this command to set the mld ssm-map static mapping source record in the global configuration mode. Use the no or default form of this command to restore the default setting.	
	ipv6 mld ssm-map static <i>access-list source-address</i>	
	no ipv6 mld ssm-map static <i>access-list source-address</i>	
	default ipv6 mld ssm-map static <i>access-list source-address</i>	
Parameter Description	Parameter	Description
	<i>access-list</i>	Sets the IPv6 ACL name.
	<i>source-address</i>	Sets the unicast address for the group record mapping.
Defaults	There is no mapping source address by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used with the ipv6 mld ssm-map enable command. With this command configured, the received mldv1 packets are mapped to the correspondent source record.	
Configuration Examples	The following example maps all group record of the ACL name to the source address 4444::1234. <pre>FS(config)# ipv6 mld ssm-map enable FS(config)# ipv6 mld ssm-map static te 4444::1234</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.17 ipv6 mld static-group

	Use this command to add an interface to a group statically. Use the no or default form of this command to restore the default setting.	
	ipv6 mld static-group <i>group-address</i>	
	no ipv6 mld static-group <i>group-address</i>	
	default ipv6 mld static-group <i>group-address</i>	
Parameter Description	Parameter	Description
	<i>group-address</i>	Sets the IPv6 non-management multicast group address.

Defaults	The interface is not added to any group statically.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to add a multicast group to the interface directly. The difference from the join-group is that the packet interaction is not necessary. Use this command when it is necessary to add a group member to the interface. It is worth mentioning that only the no ipv6 mld static-group command can be used to delete the group, but not the clear command.	
Configuration Examples	The following example adds interface Eth0/1 to group ff55::3 statically. <pre>FS# configure terminal FS(config)# interface ethernet 0/1 FS(config-if-Ethernet 0/1)# ipv6 mld static-group ff55::3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.18 ipv6 mld version

	Use this command to set the MLD version number on the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 mld version { 1 2 }	
	no ipv6 mld version	
	default ipv6 mld version	
Parameter Description	Parameter	Description
	{ 1 2 }	Sets the MLD version number.
Defaults	The default is 2.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to control the MLD version number.	
Configuration Examples	The following example sets the MLD version 1. <pre>FS# configure terminal FS(config)# interface ethernet 0/1</pre>	

	FS(config-if-Ethernet 0/1)# ipv6 mld version 1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.19 show ipv6 mld groups

	Use this command to display the group connected with the switch and the group information learned from the MLD.	
	show ipv6 mld groups [<i>group-address</i> <i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	group-address	Sets the IPv6 multicast group address in 128 bits.
	interface-type	Sets the interface type.
	interface-number	Sets the interface number.
	detail	Displays the information in detail.
		Displays all the group information.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Interface configuration mode	
Usage Guide	Use this command without the parameters to display the information including the group address, the interface type and the multicast group information. Use this command with a parameter to display the information on a specific group.	
Configuration Examples	The following example displays all group information. <pre>FS# show ipv6 mld groups MLD Connected Group Membership Group Address Interface Uptime Expires Last Reporter ff66::1 VLAN1 00:10:57 00:02:16 fe80::2d0:f8ff:fe22:3378</pre> The following example displays the detailed information. <pre>FS# show ipv6 mld groups detail Interface: VLAN 1 Group: ff66::1 Uptime: 00:10:26 Group mode: Exclude (Expires: 00:02:47) Last reporter: fe80::2d0:f8ff:fe22:3378</pre>	

	Source list is empty	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.20 show ipv6 mld interface

	Use this command to display the configurations on the interface.	
	show ipv6 mld interface [interface-type interface-number]	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Sets the interface type.
	<i>interface-number</i>	Sets the interface number.
Defaults	N/A	
Command Mode	User EXEC mode/Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the state information of all interfaces. <pre> FS# show ipv6 mld interface Interface VLAN 2 (Index 4098) MLD Enabled, Inactive, Version 2 (default) MLD interface limit is 1024 MLD interface has 0 group-record states MLD interface has 1 join-group records MLD interface has 0 static-group records MLD activity: 0 joins, 0 leaves MLD query interval is 125 seconds MLD querier timeout is 255 seconds MLD max query response time is 10 seconds Last member query response interval is 10 (1/10s) Last member query count is 2 Group Membership interval is 260 Robustness Variable is 2 </pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.21 show ipv6 mld ssm-mapping

	Use this command to display the mapping information of the source address for the group record.	
	show ipv6 mld ssm-mapping [<i>group-address</i>]	
Parameter Description	Parameter	Description
	<i>group-address</i>	Displays the group address.
Defaults	N/A	
Command Mode	User EXEC mode/Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the state information of all interfaces. <pre> FS# show ipv6 mld interface Interface VLAN 2 (Index 4098) MLD Enabled, Inactive, Version 2 (default) MLD interface limit is 1024 MLD interface has 0 group-record states MLD interface has 1 join-group records MLD interface has 0 static-group records MLD activity: 0 joins, 0 leaves MLD query interval is 125 seconds MLD querier timeout is 255 seconds MLD max query response time is 10 seconds Last member query response interval is 10 (1/10s) Last member query count is 2 Group Membership interval is 260 Robustness Variable is 2 </pre>	
Related Commands	Command	Description
	N/A	N/A

5 PIM-DM Commands

5.1 clear ip pim dense-mode track

	Use this command to clear the statistics of PIM-DM packets.	
	clear ip pim dense-mode track	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to reconfigure the start time of the statistics and clear the PIM packet counter.	
Configuration Examples	The following example clears the statistics of PIM-DM packets. FS# clear ip pim dense-mode track	
Related Commands	Command	Description
	show ip pim dense-mode track	Displays the statistics of the PIM packets.
Platform Description	N/A	

5.2 ip pim dense-mode

	Use this command to enable PIM-DM on the interface. Use the no or default form of this command to restore the default setting.	
	ip pim dense-mode	
	no ip pim dense-mode	
	default ip pim dense-mode	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	PIM-DM PASSIVE is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Please configure multicast route forwarding in global configuration mode before enabling PIM-DM PASSIVE. When PIM-DM PASSIVE is enabled, IGMP is enabled on each interface automatically. Enabled with PIM-DM PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-DM PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.	
Configuration Examples	The following example enables PIM-DM PASSIVE on interface fastethernet 0/1. <pre>FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim dense-mode passive</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.4 ip pim dense-mode subvlan

	Use this command to enable PIM-DM on the Super VLAN interface. Use the no or default form of this command is to restore the default setting.	
	ip pim dense-mode subvlan [all vid]	
	no ip pim dense-mode subvlan	
	default ip pim dense-mode subvlan	
Parameter Description	Parameter	Description
	all	Sends PIM packets to all sub VLANs.
	<i>vid</i>	Sends PIM packets to the specified VLAN.
Defaults	PIM-DM is disabled on the Super VLAN interface by default.	
Command Mode	Interface configuration mode	

Usage Guide	In general, a super VLAN includes many sub VLANs. If the PIM-DM protocol is enabled on the interfaces of the super VLAN, PIM-DM multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN interface is disabled with PIM-DM generally. Use this command to enable PIM-DM on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.	
Configuration Examples	The following example enables PIM-DM on the Super VLAN interface and sends PIM packets to sub VLAN 200. <pre>FS# configure terminal FS(config)# interface vlan 100 FS(config-if-vlan 100)# ip pim dense-mode subvlan 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.5 ip pim neighbor-filter

	Use this command to enable the neighbor filtering on the interface. Use the no or default form of this command is to restore the default setting.	
	ip pim neighbor-filter <i>access-list</i>	
	no ip pim neighbor-filter <i>access-list</i>	
	default ip pim neighbor-filter <i>access-list</i>	
Parameter Description	Parameter	Description
	<i>access-list</i>	Access control list supporting numerical ACL in the range from 1 to 99 and name ACL
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	If the neighbor filtering is set, PIM-DM will not establish the peering relationship with this neighbor or will terminate the established peering relationship with this neighbor once the neighbor is denied by the filtering access list.	
Configuration Examples	The following example enables the neighbor filtering on the interface. <pre>FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim neighbor-filter 14</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.6 ip pim override-interval

	Use this command to reconfigure the override-interval of the hello message. Use the no or default form of this command to restore the default setting.	
	ip pim override-interval <i>interval-milliseconds</i>	
	no ip pim override-interval	
	default ip pim override-interval	
Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	In the range from 1 to 65,535 in the unit of milliseconds
Defaults	The default is 2,500 milliseconds.	
Command Mode	Interface configuration mode	
Usage Guide	Configuring the override-interval is to set the pruning veto time for the interface.	
Configuration Examples	The following example sets the override-interval to 3,000 milliseconds. <pre> FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim override-interval 3000 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.7 ip pim propagation-delay

	Use this command to reconfigure the propagation-interval of the hello message. Use the no or default form of this command to restore the default setting.	
	ip pim propagation-delay <i>interval-milliseconds</i>	

	no ip pim propagation-delay	
	default ip pim propagation-delay	
Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	Propagation-interval of the hello message in the range from 1 to 32,767 in the unit of milliseconds
Defaults	The default is 500 milliseconds.	
Command Mode	Interface configuration mode	
Usage Guide	Configuring the propagation-delay is to set the transmission delay time for the interface.	
Configuration Examples	The following example sets the propagation-delay to 600 milliseconds. <pre> FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim propagation-delay 600 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.8 ip pim query-interval

	Use this command to reconfigure the interval of sending the hello message. Use the no or default form of this command to restore the default setting.	
	ip pim query-interval <i>interval-seconds</i>	
	no ip pim query-interval	
	default ip pim query-interval	
Parameter Description	Parameter	Description
	<i>interval-seconds</i>	Interval of sending the hello message in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 30 seconds.	
Command Mode	Interface configuration mode	

Usage Guide	If hello interval is set, the hello holdtime value will be updated to 3.5 times of hello interval.	
Configuration Examples	The following example sets the interval of sending the hello message to 123 seconds. <pre>FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim query-interval 123</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.9 ip pim state-refresh disable

	Use this command to prohibit the interface from processing and forwarding the PIM-DM state refresh messages. Use the no or default form of this command to restore the default setting.	
	ip pim state-refresh disable	
	no ip pim state-refresh disable	
	default ip pim state-refresh disable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the PIM-DM state refresh messages can be processed and forwarded.	
Command Mode	Global configuration mode	
Usage Guide	When the state refresh function is disabled, the PIM-DM state refresh message is not processed and forwarded. The sent Hello message does not contain the status refresh option. Consequently, the SR Cap field will not be processed when the Hello message is received. Generally, it is not recommended to disable the status refresh function because disabling this function may converge the PIM-DM multicast forwarding tree again that has been converged, resulting in unnecessary waste of bandwidth and oscillation of multicast routing table.	
Configuration Examples	The following example disables the processing of the PIM-DM state refresh message. <pre>FS# configure terminal FS(config)# ip pim state-refresh disable</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.10 ip pim state-refresh origination-interval

	Use this command to set the interval of sending the PIM-DM state refresh message. The interval is the seconds elapsed between two state refresh messages. Use the no or default form of this command to restore the default setting.	
	ip pim state-refresh origination-interval <i>interval-seconds</i>	
	no ip pim state-refresh origination-interval	
	default ip pim state-refresh origination-interval	
Parameter Description	Parameter	Description
	<i>interval-seconds</i>	Interval of sending the PIM-DM update message in the range from 1 to 100 in unit of seconds
Defaults	The default is 60 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the interval of sending the PIM-DM state refresh message to 65 seconds. <pre>FS# configure terminal FS(config)# interface fastethernet 0/1 FS(config-if)# ip pim state-refresh origination-interval 65</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.11 ip pim mib dense-mode

	Use this command to switch the device from the PIM MIB sparse mode to the PIM MIB dense mode. Use the no form or default form of this command to switch back to the PIM MIB sparse mode.	
	ip pim mib dense-mode	

	no ip pim mib dense-mode	
	default ip pim mib dense-mode	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The device is in the PIM MIB sparse mode by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example switches the device from the PIM MIB sparse mode to the PIM MIB dense mode. <pre>FS# configure terminal FS(config)# ip pim mib dense-mode</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.12 show ip pim dense-mode interface

	Use this command to display the information about the PIM-DM interface.	
	show ip pim dense-mode interface [<i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface ID
	detail	Displays details of the interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the PIM-DM interface. <pre>FS# show ip pim dense-mode interface</pre>	

	Address Interface VIFIndex Ver/Mode Nbr Mode Count 10.10.10.10 FastEthernet 0/45 3 v2/D 1 50.50.50.50 VLAN4 2 v2/D 1												
	<table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Address</td><td>Primary IP address of the PIM-DM interface</td></tr> <tr> <td>Interface</td><td>Name of the PIM-DM interface</td></tr> <tr> <td>VIF Index</td><td>VIF ID (ID)</td></tr> <tr> <td>Ver/Mode</td><td>PIM version/mode</td></tr> <tr> <td>Nbr Count</td><td>Number of neighbors of the PIM-DM interface.</td></tr> </table>	Field	Description	Address	Primary IP address of the PIM-DM interface	Interface	Name of the PIM-DM interface	VIF Index	VIF ID (ID)	Ver/Mode	PIM version/mode	Nbr Count	Number of neighbors of the PIM-DM interface.
Field	Description												
Address	Primary IP address of the PIM-DM interface												
Interface	Name of the PIM-DM interface												
VIF Index	VIF ID (ID)												
Ver/Mode	PIM version/mode												
Nbr Count	Number of neighbors of the PIM-DM interface.												
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show ip pim dense-mode neighbor</td><td>Displays the information about the neighbors of the PIM-DM interface.</td></tr> </table>	Command	Description	show ip pim dense-mode neighbor	Displays the information about the neighbors of the PIM-DM interface.								
Command	Description												
show ip pim dense-mode neighbor	Displays the information about the neighbors of the PIM-DM interface.												
Platform Description	N/A												

5.13 show ip pim dense-mode mroute

	Use this command to display the information about the PIM-DM routing table.	
	show ip pim dense-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]] [summary]	
Parameter Description	Parameter	Description
	<i>group-or-source-address</i>	Group address or source address
	<i>group-or-source-address</i>	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.
	summary	Displays the brief information of routing entries.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the PIM-Dm routing table.	
	<pre>FS# show ip pim dense-mode mroute PIM-DM Multicast Routing Table (1.1.1.111, 229.1.1.1) MRT lifetime expires in 205 seconds</pre>	

	RPF Neighbor: 50.50.50.1, Nexthop:50.50.50.1,VLAN 4 Upstream IF: VLAN 4 Upstream State: Pruned, PLT:200 Assert State: NoInfo Downstream IF List: FastEthernet 0/45: Downstream State: NoInfo Assert State: Loser, AT:170	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.14 show ip pim dense-mode neighbor

	Use this command to display the information about the PIM-DM neighbors.																								
	show ip pim dense-mode neighbor [<i>interface-type interface-number</i>]																								
Parameter Description	Parameter	Description																							
	<i>interface-type interface-number</i>	Interface type and interface ID																							
Defaults	N/A																								
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																								
Usage Guide	N/A																								
Configuration Examples	The following example displays the information about the PIM-DM neighbors. FS# show ip pim dense-mode neighbor <table><tr><td>Neighbor-Address</td><td>Interface</td><td>Uptime/Expires</td><td>Ver</td></tr><tr><td>10.10.10.1</td><td>FastEthernet 0/45</td><td>00:19:29/00:01:21</td><td>v2</td></tr><tr><td>50.50.50.1</td><td>VLAN 4</td><td>00:22:09/00:01:39</td><td>v2</td></tr></table> Description of fields in the results: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Neighbor-Address</td><td>IP address of the neighbor</td></tr><tr><td>Interface</td><td>Name of the interface connecting the neighbor</td></tr><tr><td>Uptime/Expires</td><td>Valid time and aging time of the entry</td></tr><tr><td>Ver</td><td>PIM version</td></tr></table>			Neighbor-Address	Interface	Uptime/Expires	Ver	10.10.10.1	FastEthernet 0/45	00:19:29/00:01:21	v2	50.50.50.1	VLAN 4	00:22:09/00:01:39	v2	Field	Description	Neighbor-Address	IP address of the neighbor	Interface	Name of the interface connecting the neighbor	Uptime/Expires	Valid time and aging time of the entry	Ver	PIM version
Neighbor-Address	Interface	Uptime/Expires	Ver																						
10.10.10.1	FastEthernet 0/45	00:19:29/00:01:21	v2																						
50.50.50.1	VLAN 4	00:22:09/00:01:39	v2																						
Field	Description																								
Neighbor-Address	IP address of the neighbor																								
Interface	Name of the interface connecting the neighbor																								
Uptime/Expires	Valid time and aging time of the entry																								
Ver	PIM version																								

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.15 show ip pim dense-mode nexthop

	Use this command to display the information about the PIM-DM next hop.					
	show ip pim dense-mode nexthop					
Parameter Description	Parameter			Description		
	N/A			N/A		
Defaults	N/A					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode					
Usage Guide	N/A					
Configuration Examples	The following example displays the information about the PIM-Dm next hop:					
	FS# show ip pim dense-mode nexthop					
	Destination	Nexthop	Nexthop	Nexthop	Metric	Pref
		Num	Addr	Interface		
	1.1.1.111	1	50.50.50.1	VLAN 4	0	1
	Field		Description			
	Destination		Multicast source IP address			
	Nexthop Num		Number of next hop			
	Nexthop Addr		IP address of next hop			
Nexthop interface		Interface connecting to the of next hop				
Metric		Route metric				
Pref		Route priority				
Related Commands	Command			Description		
	N/A			N/A		
Platform Description	N/A					

5.16 show ip pim dense-mode track

	Use this command to display the statistics of the PIM-DM packets.	
	show ip pim dense-mode track	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the clear ip pim dense-mode track every time.	
Configuration Examples	The following example displays the statistics of the PIM-DM packets. <pre> FS# show ip pim dense-mode track PIM packet counters Elapsed time since counters cleared: 00:04:03 received sent Valid PIMDM packets: 1 8 Hello: 1 8 Join/Prune: 0 0 Graft: 0 0 Graft-Ack: 0 0 Assert: 0 0 State-Refresh: 0 0 PIM-SM-Register: 0 0 PIM-SM-Register-Stop: 0 0 PIM-SM-BSM: 0 0 PIM-SM-C-RP-ADV: 0 0 Unknown Type: 0 Errors: Malformed packets: 0 Bad checksums: 0 Unknown PIM version: 0 Send errors: 0 </pre>	
Related Commands	Command	Description
	clear ip pim dense-mode track	Clears the statistics of the PIM packets.
Platform Description	N/A	

6 PIM-SM Commands

6.1 clear ip pim sparse-mode bsr rp-set *

	Use this command to clear all the RP information learnt dynamically.	
	clear ip pim sparse-mode bsr rp-set *	
Parameter Description	Parameter	Description
	-	-
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	All the RP information learnt dynamically can be cleared manually.	
Configuration Examples	The following example clears all the RP information learnt dynamically. FS# clear ip pim sparse-mode bsr rp-set *	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.2 clear ip pim sparse-mode track

	Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.	
	clear ip pim sparse-mode track	
Parameter Description	Parameter	Description
	-	-
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide		

Configuration	The following example clears the PIM packet counter.	
Examples	FS# clear ip pim sparse-mode track	
Related Commands	Command	Description
	show ip pim sparse-mode track	Displays the PIM packet statistics.
Platform Description	N/A	

6.3 ip pim accept-bsr list

	Use this command to confine the BSR address range. Use the no or default form this command to restore the default setting.	
	ip pim accept-bsr list <i>access-list</i>	
	no ip pim accept-bsr	
	default ip pim accept-bsr	
Parameter Description	Parameter	Description
	list <i>access-list</i>	IP standard number ACL in the range of 1 to 99, 1300 to 1999 and characters
Defaults	By default, the PIMSM router receives all external BSM packets.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to limit the range of the legal BSR.	
Configuration Examples	The following example confines the BSR address range. FS(config)# ip pim accept-bsr list 1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.4 ip pim accept-crp list

	Use this command to confine the C-RP address range and the multicast group address range it serves. Use the no or default form of this command to restore the default setting,

	ip pim accept-crp list <i>access-list</i>	
	no ip pim accept-crp	
	default ip pim accept-crp	
Parameter Description	Parameter	Description
	list <i>access-list</i>	IP extension number ACL in the range of 1 to 99, 1300 to 1999 and characters
Defaults	By default, the elected BSR receives all external advertisements of candidate RPs.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.	
Configuration Examples	The following example confines the C-RP address range and the multicast group address range it serves. FS (config)# ip pim accept-crp list 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.5 ip pim accept-crp-with-null-group

	Use this command to receive the C-RP-ADV packets whose prefix-count is 0. Use the no or default form of this command to restore the default setting.	
	ip pim accept-crp-with-null-group	
	no ip pim accept-crp-with-null-group	
	default ip pim accept-crp-with-null-group	
Parameter Description	Parameter	Description
	-	-
Defaults	By default, the BSR does not receive the C-RP-ADV packets whose prefix-count is 0.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive	

	the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.	
Configuration Examples	The following example receives the C-RP-ADV packets whose prefix-count is 0. FS (config)# ip pim accept-crp-with-null-group	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.6 ip pim accept-register list

	Use this command to confine the address range of the (S,G) entry of the register packets. Use the no or default form of this command to restore the default setting.	
	ip pim accept-register { list <i>access-list</i> [route-map <i>map-name</i>] route-map <i>map-name</i> [list <i>access-list</i>] }	
	no ip pim accept-register	
	default ip pim accept-register	
Parameter Description	Parameter	Description
	list <i>access-list</i>	Uses an extended IP access list to define the (S, G) address range. Access control list supporting numerical ACL in the range of 100 to 199 and 2000 to 2699 and name ACL.
	route-map <i>map-name</i>	Uses a route map to define the (S, G) address range.
Defaults	The (S, G) address range is not confined by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to confine the source IP address of register messages on RP.	
Configuration Examples	The following example confines the source address of register packets on the RP. FS (config)# ip pim accept-register list 100 FS (config)# access-list 100 permit ip 192.168.195.0 0.0.0.255 225.1.1.1 0.0.0.255	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.7 ip pim bsr-border

	Use this command to configure the BSR border. Use the no or default form of this command to restore the default setting.	
	ip pim bsr-border	
	no ip pim bsr-border	
	default ip pim bsr-border	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No BSR border is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.	
Configuration Examples	The following example sets the BSR border on the interface <i>g 0/3</i> <pre>FS(config)# interface gi 0/3 FS(config-if- GigabitEthernet 0/3)# ip pim bsr-border</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.8 ip pim bsr-candidate

	Use this command to configure the C-BSR. Use the no or default form of this command to restore the default setting.	
	ipv6 pim bsr-candidate <i>interface-type interface-number</i> [<i>hash-mask-length</i> [<i>priority-value</i>]]	
	no ipv6 pim bsr-candidate	
	default ip pim bsr-candidate	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and number
	<i>hash-mask-length</i>	(Optional) HASK mask length configured for electing the RP in the range from 0 to 32, The default is 10.

	<i>priority-value</i>	(Optional) Priority configured for the candidate BSR in the range from 0 to 255. The default is 64.
Defaults	No C-BSR is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	A PIM-SM domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR. This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IP address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message. The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IP address).	
Configuration Examples	The following example configures the C-BSR. <pre>FS(config)# ip pim bsr-candidate gi 0/3 30 192</pre>	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.9 ip pim dr-priority

	Use this command to set the DR priority. Use the no or default form of this command to restore the default setting.	
	ip pim dr-priority <i>priority-value</i>	
	no ip pim dr-priority	
	default ip pim dr-priority	
Parameter Description	Parameter	Description
	<i>priority-value</i>	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294.
Defaults	The default is 1.	

Command Mode	Interface configuration mode	
Usage Guide	To select a DR: If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR. If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.	
Configuration Examples	The following example sets the DR priority. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ip pim dr-priority 10000</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.10 ip pim ignore-rp-set-priority

	Use this command to ignore the RP priority. Use the no or default form of this command to restore the default setting.	
	ip pim ignore-rp-set-priority	
	no ip pim ignore-rp-set-priority	
	default ip pim ignore-rp-set-priority	
Parameter Description	Parameter	Description
	-	-
Defaults	By default, the C-RP with higher priority is selected.	
Command Mode	Global configuration mode	
Usage Guide		
Configuration Examples	The following example ignores the RP priority. <pre>FS(config)# ip pim ignore-rp-set-priority</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.11 ip pim jp-timer

	Use this command to set the interval to send the join/prune message. Use the no or default form of this command to restore the default setting.	
	ip pim jp-timer <i>seconds</i>	
	no ip pim jp-timer	
	default ip pim jp-timer	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval to send the join/prune message in the range from 1 to 65535 in the unit of seconds
Defaults	The default is 60 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the interval to send the Join/Prune message to 50 seconds. <pre>FS(config)# ip pim jp-timer 50</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.12 ip pim neighbor-filter

	Use this command to confine the neighbor address range. Use the no or default form of this command to restore the default setting.	
	ip pim neighbor-filter <i>access_list</i>	
	no ip pim neighbor-filter <i>access_list</i>	
	default ip pim neighbor-filter <i>access_list</i>	

Parameter Description	Parameter	Description
	<i>access_list</i>	Access control list supporting numerical ACL in the range 1 to 99 and name ACL
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.	
Configuration Examples	The following example blocks the neighbor address 192.168.1.5. <pre> FS(config)# interface gi 0/3 FS(config-if- GigabitEthernet 0/3)# ip pim neighbor-filter 14 FS(config-if- GigabitEthernet 0/3)# exit FS(config)# access-list 14 deny 192.168.1.5 0.0.0.255 </pre>	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.13 ip pim neighbor-tracking

	Use this command to disable join restraint on the interface. Use the no or default form of this command to restore the default setting.	
	ip pim neighbor-tracking	
	no ip pim neighbor-tracking	
	default ip pim neighbor-tracking	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	

Usage Guide	Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.	
Configuration Examples	The following example disables join restraint on the interface. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ip pim neighbor-tracking</pre>	
Related Commands	Command	Description
	ip pim propagation-delay	N/A
Platform Description	N/A	

6.14 ip pim override-interval

	Use this command to set the override-interval on the interface. Use the no or default form of this command to restore the default setting.	
	ip pim override-interval <i>milliseconds</i>	
	no ip pim override-interval	
	default ip pim override-interval	
Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	In the range from 1 to 65,535 in the unit of milliseconds
Defaults	The default is 2,500 milliseconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set the override-interval for the interface.  Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.	
Configuration Examples	The following example sets the override-interval as 3000 milliseconds. <pre>FS(config)# interface gi 0/3</pre>	

	FS(config-if-GigabitEthernet 0/3)# ip pim override-interval 3000	
Related Commands	Command	Description
	ip pim propagation-delay	N/A
Platform Description	N/A	

6.15 ip pim probe-interval

	Use this command to set the register probe interval. Use the no or default form of this command to restore the default setting.	
	ip pim probe-interval <i>seconds</i>	
	no ip pim probe-interval	
	default ip pim probe-interval	
Parameter Description	Parameter	Description
	<i>interval-seconds</i>	In the range from 1 to 65535 seconds
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.	
	 The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.	
Configuration Examples	The following example sets the probe time to 6 seconds.	
	FS(config)# ip pim probe-interval 6	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.16 ip pim propagation-delay

Use this command to set the propagation-delay on the interface.

Use the **no** or **default** form of this command to restore the default setting.

ip pim propagation-delay *milliseconds*

no ip pim propagation-delay

default ip pim propagation-delay

Parameter Description	Parameter	Description
	<i>interval-milliseconds</i>	In the range from 1 to 32,765 milliseconds

Defaults The default is 500 milliseconds.

Command Interface configuration mode

Mode

Usage Guide Use this command to set the propagation-delay for the interface.



Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

Configuration The following example sets the propagation delay to 600 milliseconds.

Examples

```
FS(config)# interface gi 0/3
FS(config)# ip pim propagation-delay 600
```

Related Commands	Command	Description
	ip pim override-interval	N/A
	ip pim neighbor-tracking	N/A

Platform N/A

Description

6.17 ip pim query-interval

	Use this command to set the interval to send the hello packets.	
	Use the no or default form of this command to restore the default setting.	
	ip pim query-interval <i>seconds</i>	
	no ip pim query-interval	
	default ip pim query-interval	
Parameter Description	Parameter	Description
	<i>interval-seconds</i>	Interval to send the Hello message, in the range from 1 to 65,535 in the unit of seconds.

Defaults	The default is 30 seconds.				
Command Mode	Interface configuration mode				
Usage Guide	Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18752.				
Configuration Examples	The following example sets the interval to send the hello packets to 123 seconds. <pre>FS(config)# interface gi 0/3 FS(config)# ip pim query-interval 123</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.18 ip pim register-checksum-wholepkt

	Use this command to calculate the checksum of the whole register packet. Use the no or default form of this command to restore the default setting.	
	ip pim register-checksum-wholepkt [group-list access-list]	
	no ip pim register-checksum-wholepkt [group-list access-list]	
	default ip pim register-checksum-wholepkt [group-list access-list]	
Parameter Description	Parameter	Description
	<i>access-list</i>	Access-list: access control list supporting numerical ACL in the range from 100 to 199 and from 1300 to 1999 and name ACL. Group-list access-list :all multicast packets use this configuration by default
Defaults	By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message	
Command Mode	Global configuration mode	
Usage Guide	Some vendors calculate checksum based on the overall registration packets. FS Networks introduces this function for the compatibility with devices of other vendors.	

Configuration	The following example calculates the checksum of the whole register packet.	
Examples	FS(config)#ip pim register-checksum-wholepkt group-list 99 FS(config)# access-list 99 permit 225.1.1.1 0.0.0.255	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.19 ip pim register-decapsulate-forward

	Use this command to enable the RP to decapsulate the register packets and forward the multicast packets. Use the no or default form of this command to restore the default setting.	
	ip pim register-decapsulate-forward	
	no ip pim register-decapsulate-forward	
	default ip pim register-decapsulate-forward	
Parameter Description	Parameter	Description
	-	-
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to implement the decapsulate of the PIM-SM registration packets with the multicast data packets received on the candidate RP and forward the multicast data packets. As the decapsulating and forwarding are performed by the software, it is not recommended to configure this command in the case that many registration packets need to be decapsulated and forwarded, which may cause the CPU busy with this function configured.	
Configuration Examples	The following example enables the RP to decapsulate the register packets and forwards the multicast packets. FS(config)# ip pim register-decapsulate-forward	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.20 ip pim register-rate-limit

	Use this command to limit the rate of register packets. Use the no form of this command to restore the default setting.	
	ip pim register-rate-limit <i>rate</i>	
	no ip pim register-rate-limit	
	default ip pim register-rate-limit	
Parameter Description	Parameter	Description
	-	-
	<i>rate</i>	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535
Defaults	By default, there is no rate limitation on register messages.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.	
Configuration Examples	The following example limits the rate of register packets. FS(config)# ip pim register-rate-limit 3000	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.21 ip pim register-rp-reachability

	Use this command to check RP reachability before sending register packets. Use the no or default form of this command to restore the default setting.	
	ip pim register-rp-reachability	
	no ip pim register-rp-reachability	
	default ip pim register-rp-reachability	
Parameter Description	Parameter	Description
	-	-

Defaults	By default, the RP reachability is not checked before sending register packets.				
Command Mode	Global configuration mode				
Usage Guide	This command is used to check the RP reachability before sending register packets. If not, register packets are not transmitted.				
Configuration Examples	The following example checks the RP reachability before sending register packets. FS(config)# ipv6 pim register-rp-reachability				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.22 ip pim register-source

	Use this command to specify the source IP address of the register packets. Use the no or default form of this command to restore the default setting.	
	ip pim register-source { <i>local_address</i> <i>interface-type interface-number</i> }	
	no ip pim register-source	
	default ip pim register-source	
Parameter Description	Parameter	Description
	-	-
	<i>interface-type interface-number</i>	Interface whose IP address is used as the source IP address of register packets
	<i>local_address</i>	Specifies the source IP address of the register packet.
Defaults	By default, the source IP address of register packets is the IP address of the DR interface connecting the multicast source.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure the source IP address of register messages. The source IP address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IP address as the destination IP address of the Register-Stop packet. It is not necessary to enable the PIM.	

Configuration Examples	The following example specifies the source IP address of the register packets. FS(config)# ip pim register-source 192.168.195.80 FS(config)# ip pim register-source gi 0/3	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.23 ip pim register-suppression

	Use this command to set the register suppression time. Use the no or default form of this command to restore the default setting.	
	ip pim register-suppression <i>seconds</i>	
	no ip pim register-suppression	
	default ip pim register-suppression	
Parameter Description	Parameter	Description
	<i>suppression</i>	Suppression time in the range from 1 to 65,535 in the unit of seconds.
Defaults	The default is 60 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Executing this command on the DR will change the register packet suppression time configured. if the ip pim rp-register-kat command is not configured, executing this command on RP will modify the period of RP keepalive.	
Configuration Examples	The following example sets the register suppression time to 100 seconds. FS(config)# ip pim register-suppression 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.24 ip pim rp-address

	Use this command to configure the static RP. Use the no or default form of this command to restore the default setting.	
	ip pim rp-address <i>rp-address</i> [<i>access_list</i>]	
	no ip pim rp-address <i>rp-address</i> [<i>access_list</i>]	
	default ip pim rp-address <i>rp-address</i> [<i>access_list</i>]	
Parameter Description	Parameter	Description
	<i>rp-address</i>	IP address of RP
	<i>access_list</i>	Access control list supporting numerical ACL in the range 1 to 99 and 1300 to 1999 and name ACL. All multicast groups are supported by default.
Defaults	No IP address is configured for the static RP by default.	
Command Mode	Global configuration mode	
Usage Guide	This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that: If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes precedence. You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once. If there are more than one static RP in a multicast group, the one of the highest IP address is used. Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted. After configuration is performed, the static RP's source IP address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IP address. When you select a RP from a static RP group, the first entry, namely the one with the largest IP address, will be selected first. Deleting a static IP address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.	
Configuration Examples	The following example specifies the source IPv6 address of the register packet. <pre>FS(config)# ip pim rp-address 210.34.0.55 4 FS(config)# access-list 4 permit 255.1.1.1 0.0.0.255</pre>	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.25 ip pim rp-candidate

	Use this command to configure the C-RP. Use the no or default form of this command to restore the default setting.	
	ip pim rp-candidate <i>interface-type interface-number</i> [priority <i>priority-value</i>] [interval <i>seconds</i>] [group-list <i>access_list</i>]	
	no ip pim rp-candidate [<i>interface-type interface-number</i>]	
	default ip pim rp-candidate [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface number
	<i>priority-value</i>	(Optional) Priority in the range 0 to 255, 192 by default
	<i>seconds</i>	(Optional) Interval in the range 0 to 16,383 seconds, 60s by default
	<i>access_list</i>	(Optional) Numerical ACL in the range 1 to 99 or name ACL. By default, all multicast groups are permitted.
Defaults	No C-RP is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	In the PIM-SM protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs send C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain. To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.	
Configuration Examples	The following example configures the C-RP. <pre>FS(config)# ip pim rp-candidate gi 0/3 priority 200 group-list 3 interval 70 FS(config)# access-list 3 permit 255.1.1.1 0.0.0.255</pre>	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.26 ip pim rp-register-kat

	Use this command to set the KAT interval on the RP. Use the no or default form of this command to restore the default setting.
	ip pim rp-register-kat <i>seconds</i>

	no ip pim rp-register-kat	
	default ip pim rp-register-kat	
Parameter Description	Parameter	Description
	<i>seconds</i>	KAT timer time in the range from 1 to 65,525 in the unit of seconds
Defaults	The default is 210 seconds.	
Command Mode	Global configuration mode	
Usage Guide		
Configuration Examples	The following example sets the KAT interval on the RP to 250 seconds. <pre>FS(config)# ip pim rp-register-kat 250</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.27 ip pim sparse-mode

	Use this command to enable PIM-SM on the interface. Use the no or default form of this command to restore the default setting.	
	ip pim sparse-mode	
	no ip pim sparse-mode	
	default ip pim sparse-mode	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to enable PIM-SM on the interface.  You need to enable multicast routing forwarding in the global configuration mode before enabling	

	PIM-SM. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.  During the execution of this command, if the prompt "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.  During the execution of this command, if the prompt "PIM-SM Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SM on the interface, delete the unnecessary PIM-SM, PIM-DM or DVMRP interfaces. 					
Configuration Examples	The following example enables PIM-SM on the interface. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ip pim sparse-mode</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

6.28 ip pim sparse-mode passive

	Use this command to enable PIM-SM PASSIVE. Use the no or default form of this command to restore the default setting.	
	ip pim sparse-mode passive	
	no ip pim sparse -mode passive	
	default ip pim sparse-mode passive	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	PIM-SM PASSIVE is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Please configure multicast route forwarding in global configuration mode before enabling PIM-SM PASSIVE. When PIM-SM PASSIVE is enabled, IGMP is enabled on each interface automatically. Enabled with PIM-SM PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-SM PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.	
Configuration	The following example enables PIM-SM PASSIVE on interface GigabitEthernet 0/3.	

Examples	<pre>FS# configure terminal FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ip pim sparse-mode passive</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.29 ip pim sparse-mode subvlan

	Use this command to enable PIM-SM on the Super VLAN interface. Use the no or default form of this command is to restore the default setting.	
	ip pim sparse-mode subvlan [all vid]	
	no ip pim sparse-mode subvlan	
	default ip pim sparse-mode subvlan	
Parameter Description	Parameter	Description
	all	Sends PIM packets to all sub VLANs.
	<i>vid</i>	Sends PIM packets to the specified VLAN.
Defaults	PIM-SM is disabled on the Super VLAN interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	In general, a super VLAN includes many sub VLANs. If the PIM-SM protocol is enabled on the interfaces of the super VLAN, PIM-SM multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN interface is disabled with PIM-SM generally. Use this command to enable PIM-SM on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.	
Configuration Examples	The following example enables PIM-SM on the Super VLAN interface and sends PIM packets to sub VLAN 200. <pre>FS# configure terminal FS(config)# interface vlan 100 FS(config-if-vlan 100)# ip pim sparse-mode subvlan 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.30 ip pim spt-threshold

	Use this command to enable the SPT switching function. Use the no or default form of this command to restore the default setting.	
	ip pim spt-threshold [group-list <i>access-list</i>]	
	no ip pim spt-threshold [group-list <i>access-list</i>]	
	default ip pim spt-threshold [group-list <i>access-list</i>]	
Parameter Description	Parameter	Description
	<i>access_list</i>	(Optional) Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL. By default, all multicast groups are permitted for SPT switching.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using group-list) or all multicast groups (not using group-list) .	
Configuration Examples	The following example enables the SPT switching function. <pre>FS(config)# ip pim spt-threshold group-list 12 FS(config)# access-list 12 permit 225.1.1.1 0.0.0.255</pre>	
Related Commands	Command	Description
	access-list	N/A
Platform Description	N/A	

6.31 ip pim ssm

	Use this command to enable SSM and set the SSM group address range. Use the no or default form of this command to restore the default setting.	
	ip pim ssm { default range <i>access_list</i> }	
	no ip pim ssm	
	default ip pim ssm	
Parameter Description	Parameter	Description
	default	Multicast groups of 232/8
	range <i>access_list</i>	Numerical ACL in the range 1 to 99 and 1300 to 1999 or name ACL.

Defaults	This function is disabled by default.				
Command Mode	Global configuration mode				
Usage Guide	This command is used to enable PIM-SSM (or in some specific multicast groups).				
Configuration Examples	The following command enables SSM and sets the SSM group range to 232/8: <pre>FS(config)# ip pim ssm default</pre> The following command sets the source-specific multicast with ACL 10. <pre>FS(config)# ip pim ssm range 10</pre> <pre>FS(config)# access-list 10 permit 232.0.0.1 0.0.0.255</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.32 ip pim triggered-hello-delay

	Use this command to configure Triggered-Hello-Delay time on the interface. Use the no or default form of this command to restore the default setting.	
	ip pim triggered-hello-delay <i>seconds</i>	
	no ip pim triggered-hello-delay	
	default ip pim triggered-hello-delay	
Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 5 in the unit of seconds.
Defaults	The default is 5 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message in random time.	
Configuration Examples	The following command sets the triggered-hello-delay to 3 seconds. <pre>FS(config)# interface gi 0/3</pre>	

	FS(config-if-GigabitEthernet 0/3)# ip pim triggered-hello-delay 3	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.33 show debugging

Use this command to display the debugging status.

show debugging

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide		
Configuration Examples	The following example displays the debugging status. <pre>FS#show debugging ip packet debug: ip packet debug debugging is on, acl: 0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.34 show ip pim sparse-mode bsr-router

	Use this command to display the BSR information	
	show ip pim sparse-mode bsr-router	
Parameter Description	Parameter	Description
	-	-

Defaults	N/A				
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode				
Usage Guide					
Configuration Examples	The following example displays BSR information. <pre> FS# show ip pim sparse-mode bsr-router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 192.168.127.1 Uptime: 01d23h14m, BSR Priority: 64, Hash mask length: 10 Next bootstrap message in 00:00:42 Role: Candidate BSR Priority: 64, Hash mask length: 10 State: Elected BSR Candidate RP: 30.30.100.200(GigabitEthernet 0/3) Advertisement interval 60 seconds 00:00:32 </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.35 show ip pim sparse-mode interface

	Use this command to display PIM-SM interface information.	
	show ip pim sparse-mode interface [<i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
	detail	(Optional) Displays the details of an interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	

Usage Guide		
Configuration Examples	The following example displays the PIM-SM information on the interface. <pre>FS#show ip pim sparse-mode interface detail GigabitEthernet 0/3 (vif 3): Address 30.30.100.200, DR 30.30.100.200 Hello period 30 seconds, Next Hello in 11 seconds Triggered Hello period 5 seconds Neighbors: 2.2.2.2</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.36 show ip pim sparse-mode local-members

	Use this command to display the local IGMP information on the PIM-SM interface.	
	show ip pim sparse-mode local-members [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide		
Configuration Examples	The following example displays the local IGMP information on the PIM-SM interface. <pre>FS (config-if)#sh ip pim sparse-mode local-members PIM Local membership information GigabitEthernet 0/3: (*, 225.1.1.1) : Include Loopback 1: GigabitEthernet 0/5:</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.37 show ip pim sparse-mode mroute

	Use this command to display the PIM-SM routing information.	
	show ip pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]]	
Parameter Description	Parameter	Description
	<i>group-or-source-address</i>	Group IP address or source IP address. Two addresses cannot both be the group addresses or the source addresses.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	This command is used to display routing information. Only one group IP address, one source IP address or one group IP address-source IP address pair can be configured at a time. You can also specify no group IP address or source IP address.	
Configuration Examples	The following example displays the PIM-SM routing information. FS#show ip pim sparse-mode mroute	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.38 show ip pim sparse-mode neighbor

	Use this command to display the neighbor information.	
	show ip pim sparse-mode neighbor [detail]	
Parameter Description	Parameter	Description
	detail	(Optional) Displays the details of an interface.

Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide		
Configuration Examples	The following example displays the neighbor information. <pre>FS# show ip pim sparse-mode neighbor</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.39 show ip pim sparse-mode nexthop

	Use this command to display the next-hop information, including the interface ID, address and metric.	
	show ip pim sparse-mode nexthop	
Parameter Description	Parameter	Description
	-	-
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the next-hop information. <pre>FS# show ip pim sparse-mode nexthop</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.40 show ip pim sparse-mode rp mapping

	Use this command to display the information on all RPs and the multicast groups they serve.	
	show ip pim sparse-mode rp mapping	
Parameter Description	Parameter	Description
	<i>mapping</i>	All group and RP information
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information on all RPs and the multicast groups they serve. <pre> FS# show ip pim sparse-mode rp mapping PIM Group-to-RP Mappings Group(s): 224.0.0.0/4 RP: 30.30.200.1 Info source: 30.30.200.1, via bootstrap, priority 192 Uptime: 00:00:51, expires: 00:01:39 RP: 30.30.100.1 Info source: 30.30.200.1, via bootstrap, priority 192 Uptime: 00:19:14, expires: 00:01:38 Group(s): 224.0.0.0/4, Static RP: 100.100.100.100 Uptime: 00:45:35 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.41 show ip pim sparse-mode rp-hash

	Use this command to display the RP information corresponding to the group address.
	show ip pim sparse-mode rp-hash <i>group-address</i>

Parameter Description	Parameter	Description
	<i>group-address</i>	Group address to be resolved
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide		
Configuration Examples	The following example displays the RP information corresponding to the group address. <pre>FS# show ip pim sparse-mode rp-hash 255.1.1.1 RP: 30.30.100.1 Info source: 30.30.100.1, via bootstrap</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.42 show ip pim sparse-mode track

	Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.	
	show ip pim sparse-mode track	
Parameter Description	Parameter	Description
	-	-
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIM packet counter is cleared on calling the clear ip pim sparse-mode track every time.	
Configuration	The following example displays the number of sent and received PIM packets during the period from the	

Examples	beginning of the statistics till now.	
	FS # show ip pim sparse-mode track	
	PIM packet counters track	
	Elapsed time since counters cleared: 00:04:03	
	received sent	
	Valid PIMSM packets:	0 8
	Hello:	0 8
	Join-Prune:	0 0
	Register:	0 0
	Register-Stop:	0 0
	Assert:	0 0
	BSM:	0 0
	C-RP-ADV:	0 0
	PIMDM-Graft:	0
	PIMDM-Graft-Ack :	0
	PIMDM-State-Refresh:	0
	Unknown PIM Type:	0
	Errors:	
	Malformed packets:	0
	Bad checksums:	0
Send errors:	0	
Packets received with unknown PIM version:	0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7 PIM-SMv6 Commands

7.1 clear ipv6 mroute

	Use this command to clear multicast routing entries.	
	clear ipv6 mroute { * <i>ipv6_group_address</i> [<i>ipv6_source_address</i>] }	
Parameter Description	Parameter	Description
	*	Deletes all the multicast routing entries.
	<i>ipv6_group_address</i>	Deletes the multicast routing entries of the specific group.
	<i>ipv6_source_address</i>	Deletes the multicast routing entries of the specific group and source IPv6 address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears all the multicast routing entries. <pre>FS# clear ipv6 mroute *</pre> The following example clears the multicast routing entries of the specified group. <pre>FS# clear ipv6 mroute ff66::6666</pre> The following example clears the multicast routing entries of the specified group and source address. <pre>FS# clear ipv6 mroute ff66::6666 3333::3333</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.2 clear ipv6 mroute statistics

	Use this command to delete the statistics of the multicast routing entries.	
	clear ipv6 mroute statistics { * <i>ipv6_group_address</i> [<i>ipv6_source_address</i>] }	
Parameter Description	Parameter	Description
	*	Deletes the statistics of all multicast routing entries.

	<i>ipv6_group_address</i>	Deletes the statistics of the multicast routing entries of the specific group.
	<i>ipv6_source_address</i>	Deletes the statistics of the multicast routing entries of the specific group and source IPv6 address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example deletes the statistics of the multicast routing entries. <pre>FS# clear ipv6 mroute statistics *</pre> The following example clears the statistics of the multicast routing entries of the specified group. <pre>FS# clear ipv6 mroute statistics ff66::6666</pre> The following example clears the statistics of the multicast routing entries of the specified group and source address. <pre>FS# clear ipv6 mroute statistics ff66::6666 3333::3333</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.3 clear ipv6 pim sparse-mode bsr rp-set *

	Use this command to clears the RP information learnt dynamically.	
	clear ipv6 pim sparse-mode bsr rp-set *	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Only the RP information learnt dynamically can be cleared manually.	
Configuration Examples	The following example clears the RP information learnt dynamically. <pre>FS# clear ipv6 pim sparse-mode bsr rp-set *</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.4 clear ipv6 pim sparse-mode track

	Use this command to reconfigure the start time of the statistics and clear the PIMv6 packet counter.	
	clear ipv6 pim sparse-mode track	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears the PIMv6 packet counter. FS# clear ipv6 pim sparse-mode track	
Related Commands	Command	Description
	show ipv6 pim sparse-mode track	N/A
Platform Description	N/A	

7.5 ipv6 pim accept-bsr list

	Use this command to confine the BSR address range.
	Use the no or default form this command to restore the default setting.
	ipv6 pim accept-bsr list <i>ipv6_access-list</i>
	no ipv6 pim accept-bsr
	default ipv6 pim accept-bsr

Parameter Description	Parameter	Description
	list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL
Defaults	By default, the PIM-SMv6 router receives all external BSM packets.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example confines the BSR address range. <pre>FS(config)# ipv6 pim accept-bsr list bsr-list</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.6 ipv6 pim accept-crp list

	Use this command to confine the C-RP address range and the multicast group address range it serves. Use the no or default form of this command to restore the default setting,	
	ipv6 pim accept-crp list <i>ipv6_access-list</i>	
	no ipv6 pim accept-crp	
	default ipv6 pim accept-crp-with-null-group	
Parameter Description	Parameter	Description
	list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL
Defaults	No address is filtered by default.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to limit the address range of the legal C-RP and the multicast group range it serves.	
Configuration Examples	The following example confines the C-RP address range and the multicast group address range it serves. <pre>FS (config)# ipv6 pim accept-crp list crp-list</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 ipv6 pim accept-crp-with-null-group

	Use this command to receive the C-RP-ADV packets whose prefix-count is 0. Use the no or default form of this command to restore the default setting.	
	ipv6 pim accept-crp-with-null-group	
	no ipv6 pim accept-crp-with-null-group	
	default ipv6 pim accept-crp-with-null-group	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured on the candidate BSR, when this BSR becomes the elected BSR, it is able to receive the C-RP-ADV packets whose prefix-count is 0, and considers this C-RP supports all groups.	
Configuration Examples	The following example receives the C-RP-ADV packets whose prefix-count is 0. <pre>FS (config)# ipv6 pim accept-crp-with-null-group</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.8 ipv6 pim accept-register

	Use this command to accept specific register packets at the RP. Use the no or default form of this command to restore the default setting.	
	ipv6 pim accept-register { list <i>ipv6_access-list</i> [route-map <i>map-name</i>] route-map <i>map-name</i> [list <i>ipv6_access-list</i>] }	
	no ipv6 pim accept-register	

	default ipv6 pim accept-register	
Parameter Description	Parameter	Description
	list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL
	route-map <i>map-name</i>	Defines the routing map rule
Defaults	All register packets are received by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to confine the source IPv6 address of register messages on RP. If the unauthorized register source is received, the RP will return the Register-Stop message immediately.	
Configuration Examples	The following example denies register packets of the specified source address at the RP. <pre>FS(config)# ipv6 pim accept-register list register-access-list FS(config)# ipv6 access-list register-access-list FS(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any</pre>	
Platform Description	N/A	

7.9 ipv6 pim bsr-border

	Use this command to configure the BSR border. Use the no or default form of this command to restore the default setting.	
	ipv6 pim bsr-border	
	no ipv6 pim bsr-border	
	default ipv6 pim bsr-border	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No BSR border is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM packets upon receiving them and the BSM packets are not forwarded from this interface.	
Configuration	The following example sets the BSR border on the interface <i>gi 0/3</i> .	

Examples	FS(config)# interface gi 0/3	
	FS(config-if-GigabitEthernet)# ipv6 pim bsr-border	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.10 ipv6 pim bsr-candidate

	Use this command to configure the candidate bootstrap router (C-BSR). Use the no or default form of this command to restore the default setting.	
	ipv6 pim bsr-candidate <i>interface-type interface-number</i> [<i>hash-mask-length</i> [<i>priority-value</i>]]	
	no ipv6 pim bsr-candidate	
	default ipv6 pim bsr-candidate	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and number.
	<i>hash-mask-length</i>	(Optional) HASK mask length configured for electing the RP in the range from 0 to 128. The default is 126.
	<i>priority-value</i>	(Optional) Priority configured for the C-BSR in the range from 0 to 255. The default is 64.
Defaults	No C-BSR is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	A PIM-SMv6 domain must contain a unique BootStrap Router (BSR). BSR is responsible for collect and issue RP information. A unique recognized BSR is elected among multiple candidate BSRs through the bootstrap packet. Before BSR information is available, C-BSRs consider them to be the BSR, and regularly send bootstrap packets using the multicast address 224.0.0.13 in the PIM-SM domain. This packet contains the address and priority of the BSR. This command allows the device to send a bootstrap message to all the PIM neighbors using the assigned BSR address. Each neighbor compares the original BSR address with the address in the received bootstrap message. If the IPv6 address of the received address is equal to or larger than the original address, each neighbor saves this received address as the BSR address. Otherwise, they will discard this message. The current device considers itself to be BSR until it receives a bootstrap message from another candidate BSR and is notified that it has a higher priority value (or the same priority value, but with a larger IPv6 address).	
Configuration	The following example s configures the C-BSR.	

Examples	FS(config)# ipv6 pim bsr-candidate gi 0/3 30 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.11 ipv6 pim dr-priority

	Use this command to configure the DR priority. Use the no or default form of this command to restore the default setting.	
	ipv6 pim dr-priority <i>priority-value</i>	
	no ipv6 pim dr-priority	
	default ipv6 pim dr-priority	
Parameter Description	Parameter	Description
	<i>priority-value</i>	The larger the value, the higher the priority is. The range is from 0 to 4,294,967,294. The default is 1.
Defaults	The default is 1.	
Command Mode	Interface configuration mode	
Usage Guide	To select a DR: ● If the priority parameter of the Hello message is set for the devices in a LAN, the one of the highest priority is elected to be the DR. If several devices have the same priority, the one of the largest IP address is elected to be the DR. ● If the priority parameter of the Hello message is not set for the devices in a LAN, the one of the largest IP address is elected to be the DR.	
Configuration Examples	The following example configures the DR priority. <pre>FS(config)# interface gi 0/3 FS(config-if)# ipv6 pim dr-priority 11234</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.12 ipv6 pim ignore-rp-set-priority

	Use this command to ignore the RP priority. Use the no or default form of this command to restore the default setting.	
	ipv6 pim ignore-rp-set-priority	
	no ipv6 pim ignore-rp-set-priority	
	default ipv6 pim ignore-rp-set-priority	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the C-RP with a higher priority is selected.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example ignores the RP priority. FS(config-if)# ipv6 pim ignore-rp-set-priority	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.13 ipv6 pim jp-timer

	Use this command to set the interval to send the join/prune message. Use the no or default form of this command to restore the default setting.	
	ipv6 pim jp-timer <i>seconds</i>	
	no ipv6 pim jp-timer	
	default ipv6 pim jp-timer	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval to send the join/prune message in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 60 seconds.	

Command Mode	Global configuration mode	
Usage Guide		
Configuration Examples	The following example sets the interval to send the Join/Prune message to 100 seconds. <pre>FS# configure terminal FS(config)# ipv6 pim jp-timer 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.14 ipv6 pim neighbor-filter

	Use this command to confine the neighbor address range. Use the no or default form of this command to restore the default setting.	
	ipv6 pim neighbor-filter <i>ipv6_access-list</i>	
	no ipv6 pim neighbor-filter <i>ipv6_access-list</i>	
	default ipv6 pim neighbor-filter <i>ipv6_access-list</i>	
Parameter Description	Parameter	Description
	<i>ipv6_access_list</i>	IPv6 ACL supporting named ACL
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Neighbor filtering can enhance the security of a PIM-enabled network and provide neighbor restriction. As long as a neighbor is denied by the access list, PIM-SM will not establish the peering relationship with this neighbor or terminate the established peering relationship with this neighbor.	
Configuration Examples	The following example blocks the neighbor address fe80::2d0:f8ff:fe22:33ad. <pre>FS(config)# interface gi 0/3 FS(config-if- GigabitEthernet 0/3)# ipv6 pim neighbor-filter acl FS(config-if- GigabitEthernet 0/3)# exit FS(config)# ipv6 access-list acl FS(config-ipv6-acl)# deny ipv6 fe80::2d0:f8ff:fe22:33ad/128 any</pre>	

Related Commands	Command	Description
	ipv6_access-list	N/A
Platform Description	N/A	

7.15 ipv6 pim neighbor-tracking

	Use this command to disable join restraint on the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 pim neighbor-tracking	
	no ipv6 pim neighbor-tracking	
	default ipv6 pim neighbor-tracking	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to disable join restraint on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages.	
Configuration Examples	The following example disables join restraint on the interface. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet)# ipv6 pim neighbor-tracking</pre>	
Related Commands	Command	Description
	ipv6 pim propagation-delay	N/A
Platform Description	N/A	

7.16 ipv6 pim override-interval

	Use this command to set the override-interval on the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 pim override-interval <i>milliseconds</i>	
	no ipv6 pim override-interval	
	default ipv6 pim override-interval	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	In the range 1 to 65,535 in the unit of milliseconds
Defaults	The default is 2,500 milliseconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set the override-interval for the interface.  Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.	
Configuration Examples	The following example sets the override-interval to 3,000 milliseconds. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet)# ipv6 pim override-interval 3000</pre>	
Related Commands	Command	Description
	ipv6 pim propagation-delay	N/A
Platform Description	N/A	

7.17 ipv6 pim probe-interval

	Use this command to set the register probe interval. Use the no or default form of this command to restore the default setting.	
	ipv6 pim probe-interval <i>seconds</i>	
	no ipv6 pim probe-interval	
	default ipv6 pim probe-interval	

Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the registration probe time. The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is called probe time of null registration packet.  The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.	
Configuration Examples	The following example sets the probe time as 6 seconds. <pre>FS(config)# ipv6 pim probe-interval 6</pre>	
Related Commands	Command	Description
	ipv6 pim register-suppression	N/A
Platform Description	N/A	

7.18 ipv6 pim propagation-delay

	Use this command to set the propagation-delay on the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 pim propagation-delay <i>milliseconds</i>	
	no ipv6 pim propagation-delay	
	default ipv6 pim propagation-delay	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	In the range from 1 to 32,765 in the unit of milliseconds
Defaults	The default is 500 milliseconds.	
Command Mode	Interface configuration mode	

Usage Guide	Use this command to set the propagation-delay for the interface.  Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.	
Configuration Examples	The following example sets the propagation delay to 600 milliseconds. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ipv6 pim propagation-delay 600</pre>	
Related Commands	Command	Description
	ipv6 pim override-interval	N/A
	ipv6 pim neighbor-tracking	N/A
Platform Description	N/A	

7.19 ipv6 pim query-interval

	Use this command to set the interval to send the hello packets. Use the no or default form of this command to restore the default setting.	
	ipv6 pim query-interval <i>seconds</i>	
	no ipv6 pim query-interval	
	default ipv6 pim query-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval to send the Hello message in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 30.	
Command Mode	Interface configuration mode	
Usage Guide	Upon updating the interval to send the Hello message, the time of holding the Hello message is updated by the following principle: The hold time is updated to be 3.5 times the transmission interval. If the transmission interval*3.5 is more than 65535, the hold time is updated to 18725.	
Configuration Examples	The following example sets the interval to send the hello packets. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ipv6 pim query-interval 60</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.20 ipv6 pim register-checksum-wholepkt

	Use this command to calculate the checksum of the whole register packet. Use the no or default form of this command to restore the default setting.	
	ipv6 pim register-checksum-wholepkt [group-list <i>ipv6_access-list</i>]	
	no ipv6 pim register-checksum-wholepkt [group-list <i>ipv6_access-list</i>]	
	default ipv6 pim register-checksum-wholepkt [group-list <i>ipv6_access-list</i>]	
Parameter Description	Parameter	Description
	group-list <i>ipv6_access-list</i>	IPv6 ACL supporting named ACL. <i>ipv6_access-list</i> :all multicast packets use this configuration by default
Defaults	By default, the checksum of register messages calculates the head of PIM message and register message rather than the whole PIM message.	
Command Mode	Global configuration mode	
Usage Guide	Some vendors calculate checksum based on the overall registration packets. FS Networks introduces this function for the compatibility with these vendors.	
Configuration Examples	The following example calculates the checksum of the whole register packet. <pre>FS(config)#ipv6 pim register-checksum-wholepkt group-list checksum-access-list FS(config)# ipv6 access-list 99 checksum-access-list FS(config-ipv6-acl)# permit ipv6 any ff66::6666/64</pre>	
Related Commands	Command	Description
	ipv6 access-list	N/A
Platform Description	N/A	

7.21 ipv6 pim register-rate-limit

	Use this command to limit the rate of register packets. Use the no or default form of this command to restore the default setting.

	ipv6 pim register-rate-limit <i>rate</i>	
	no ipv6 pim register-rate-limit	
	default ipv6 pim register-rate-limit	
Parameter Description	Parameter	Description
	<i>rate</i>	Maximum number of register packets that can be sent per second, in the range from 1 to 65,535.
Defaults	By default, there is no rate limitation on register messages.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure speed of transmitting register packet in each (S, G) status, not the speed of transmitting register packets in the system. Using this command will decrease the load of source DR and RP. The register packets can be transmitted at the speed within the limit.	
Configuration Examples	The following example limits the rate of register packets.	
	FS(config)# ipv6 pim register-rate-limit 3000	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.22 ipv6 pim register-rp-reachability

	Use this command to check RP reachability before sending register packets. Use the no or default form of this command to restore the default setting.	
	ipv6 pim register-rp-reachability	
	no ipv6 pim register-rp-reachability	
	default ipv6 pim register-rp-reachability	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the RP reachability is not checked before sending register packets.	
Command Mode	Global configuration mode	

Usage Guide	This command is used to check the RP reachability before transmission. If not, register packets are not transmitted.	
Configuration Examples	The following example checks the RP reachability before sending register packets. FS(config)# ipv6 pim register-rp-reachability	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.23 ipv6 pim register-source

	Use this command to specify the source IPv6 address in the register packets. Use the no or default form of this command to restore the default setting.	
	ipv6 pim register-source { <i>ipv6_local_address</i> <i>interface-type interface-number</i> }	
	no ipv6 pim register-source	
	default ipv6 pim register-source	
Parameter Description	Parameter	Description
	<i>ipv6_local_address</i>	Source IPv6 address of register packets
	<i>interface-type interface-number</i>	Interface whose IPv6 address is used as the source IPv6 address of register packets
Defaults	By default, the source IPv6 address of register packets is the IPv6 address of the DR interface connecting the multicast source.	
Command Mode	Global configuration mode	
Usage Guide	The source IPv6 address must be reachable. When RP receives the register packet, it transmits Register-Stop packet, using its source IPv6 address as the destination IPv6 address of the Register-Stop packet.  It is not necessary to enable the PIM-SMv6 on the associated interfaces.	
Configuration Examples	The following example configures the source IPv6 address of register messages. FS(config)# ipv6 pim register-source 3333::3333 FS(config)# ipv6 pim register-source gi 0/3	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.24 ipv6 pim register-suppression

	Use this command to set the register suppression time. Use the no or default form of this command to restore the default setting.	
	ipv6 pim register-suppression <i>seconds</i>	
	no ipv6 pim register-suppression	
	default ipv6 pim register-suppression	
Parameter Description	Parameter	Description
	<i>seconds</i>	Suppression time in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 60 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Executing this command on the DR will change the register packet suppression time configured. if the ipv6 pim rp-register-kat command is not configured, executing this command on RP will modify the period of RP keepalive.	
Configuration Examples	The following example sets the register packet suppression time. <pre>FS(config)# ipv6 pim register-suppression 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.25 ipv6 pim rp embedded

	Use this command to enable the embedded RP function. Use the no or default form of this command to disable this function.	
	ipv6 pim rp embedded [<i>group-list</i> <i>ipv6_acl_name</i>]	
	no ipv6 pim rp embedded	
	default ipv6 pim rp embedded	

Parameter Description	Parameter	Description
	group-list <i>ipv6_acl_name</i>	IPv6 ACL
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable the embedded RP function explicitly and to enable the embedded RP for the IPv6 multicast address of specified embedded RP address.	
Configuration Examples	The following example enables the embedded RP for the IPv6 multicast addresses of all embedded RP addresses. FS(config)# ipv6 pim rp embedded	
Related Commands	Command	Description
	ipv6 access-list	N/A
Platform Description	N/A	

7.26 ipv6 pim rp-address

	Use this command to configure the static RP. Use the no or default form of this command to restore the default setting.	
	ipv6 pim rp-address <i>ipv6_rp-address</i> [<i>ipv6_access-list</i>]	
	no ipv6 pim rp-address <i>ipv6_rp-address</i> [<i>ipv6_access-list</i>]	
	default ipv6 pim rp-address <i>ipv6_rp-address</i> [<i>ipv6_access-list</i>]	
Parameter Description	Parameter	Description
	<i>ipv6_rp-address</i>	IPv6 address of RP
	<i>ipv6_access-list</i>	IPv6 ACL supporting named ACL
Defaults	No IPv6 address is configured for the static RP by default.	
Command Mode	Global configuration mode	
Usage Guide	This system supports the configuration of multicast static RP, as well as the configuration of static RP and BSR mechanisms at the same time. When you use this command, note that: ● If both the BSR mechanism and the static RP configuration take effect, the dynamic configuration takes	

	precedence. ● You can configure multiple multicast groups (using ACL) or all multicast groups (not using ACL) for the static RP. But a static RP can be configured only once. ● If there are more than one static RP in a multicast group, the one of the highest IPv6 address is used. ● Only the addresses permitted by ACL are valid multicast groups. By default, all the multicast groups 224/4 are permitted. ● After configuration is performed, the static RP's source IPv6 address is inserted to the group range-based static RP group tree structure. Each group range-based static multicast group maintains the chain list structure of a static RP group. This chain list is sorted in descending order of IPv6 address. When you select a RP from a static RP group, the first entry, namely the one with the largest IPv6 address, will be selected first. Deleting a static IPv6 address also deletes this address from all the existing static RP groups and selects one from in the existing RP group tree structure as the RP address.	
Configuration Examples	The following example configures the RP static address. <pre>FS(config)# ipv6 pim rp-address 3333::3333 acl FS(config)# ipv6 access-list acl FS(config)# permit ipv6 any ff66::6666/64</pre>	
Related Commands	Command	Description
	ipv6 access-list	N/A
Platform Description	N/A	

7.27 ipv6 pim rp-candidate

	Use this command to configure the candidate RP (C-RP).	
	Use the no or default form of this command to restore the default setting.	
	ipv6 pim rp-candidate <i>interface-type interface-number</i> [priority <i>priority-value</i>] [interval <i>interval-seconds</i>] [group-list <i>ipv6_access-list</i>]	
	no ipv6 pim rp-candidate [<i>interface-type interface-number</i>]	
	default ipv6 pim rp-candidate [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface number
	<i>priority-value</i>	(Optional) Priority in the range from 0 to 255, 192 by default
	<i>interval-seconds</i>	(Optional) Interval in the range from 0 to 16383 in the unit of seconds, 60 by default
	<i>ipv6_access_list</i>	(Optional) IPv6 ACL supporting named ACL
Defaults	N/A	

Command Mode	Global configuration mode	
Usage Guide	In the PIM-SMv6 protocol, the shared tree RPT created by the multicast routing uses the Rendezvous Point (RP) as the root node. RP is elected by the candidate RPs. After BSR is elected, all C-RPs sends C-RP messages in the unicast form to BSR regularly, and BSR spreads the messages throughout the PIM domain. To specify an interface as the candidate RP of a specific group, execute this command with ACL. Note that the group range is calculated only based on the permit rule, not the deny rule.	
Configuration Examples	The following example configures the RP candidate. <pre>FS(config)# ipv6 pim rp-candidate gi 0/3 priority 200 group-list acl interval 40 FS(config)# ipv6 access-list acl FS(config-ipv6-acl)# permit ipv6 any ff66::6666/64</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.28 ipv6 pim rp-register-kat

	Use this command to set the Keepalive Timer (KAT) of a (S, G) entry created by the register packet at the RP. Use the no or default form of this command to restore the default setting.	
	ipv6 pim rp-register-kat <i>seconds</i>	
	no ipv6 pim rp-register-kat	
	default ipv6 pim rp-register-kat	
Parameter Description	Parameter	Description
	<i>seconds</i>	KAT value in the range from1 to 65,525 in the unit of seconds.
Defaults	The default is equal to the sum of register probe time and three times register suppression time.	
Command Mode	Global configuration mode	
Usage Guide	The KAT value at the RP should be greater than three times the register suppression time at the source DR. Otherwise, the KAT will end and the entry (S,G) will time out before another register packet is sent, so that multicast stream will break down in a short while.	
Configuration Examples	The following example configures the KAT interval of RP. FS(config)# ipv6 pim rp-register-kat 250	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.29 ipv6 pim sparse-mode

	Use this command to enable PIM-SMv6 on the interface. Use the no or default form of this command to restore the default setting.	
	ipv6 pim sparse-mode	
	no ipv6 pim sparse-mode	
	default ipv6 pim sparse-mode	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to enable PIM-SMv6 on the interface.  You need to enable multicast routing forwarding in the global configuration mode before enabling PIM-SMv6. Otherwise, multicast packets cannot be forwarded even though you enable PIM-SM.  During the execution of this command, if the prompt "Failed to enable PIM-SMv6 on <Interface Name>, resource temporarily unavailable, please try again" appears, re-execute this command.  During the execution of this command, if the prompt "PIM-SMv6 Configure failed! VIF limit exceeded in NSM!!!" appears; it indicates the allowed configured interface number exceeds the upper limit of the multicast interfaces. In this case, if you still need to enable PIM-SMv6 on the interface, delete the unnecessary PIM-SMv6, or PIM-DMv6 interfaces.  If the interface is of tunnel-type, only 6Over4 configuration tunnel, 6Over GRE tunnel, 6Over4 configuration tunnel and 6Over6 GRE tunnel support the IPv6 multicasting at the moment. The multicasting can also be enabled on other tunnel interfaces which do not support the multicasting, but no error message will be displayed and no multicast packets will be received and forwarded.  The multicast tunnel can only be built on the Ethernet interface, the nested tunnel and the multicast data Qos/ACL are not supported.  IPv6 multicast packets cannot be forwarded through SuperVLAN.	

Configuration Examples	The following example enables PIM-SMv6 on the interface. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.30 ipv6 pim sparse-mode passive

	Use this command to enable PIM-SMv6 PASSIVE. Use the no or default form of this command to restore the default setting.	
	ipv6 pim sparse-mode passive	
	no ipv6 pim sparse -mode passive	
	default ipv6 pim sparse-mode passive	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	PIM-SMv6 PASSIVE is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Please configure multicast route forwarding in global configuration mode before enabling PIM-SMv6 PASSIVE. When PIM-SMv6 PASSIVE is enabled, IGMP is enabled on each interface automatically. Enabled with PIM-SMv6 PASSIVE, the interface neither receives nor sends PIM packets. Instead, it forwards multicast packets. PIM-SMv6 PASSIVE is generally configured on the device of the stub area, so as to avoid floods of PIM hello packets.	
Configuration Examples	The following example enables PIM-SMv6 PASSIVE on interface GigabitEthernet 0/3. <pre>FS# configure terminal FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ipv6 pim sparse-mode passive</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

7.31 ipv6 pim sparse-mode subvlan

	Use this command to enable PIM-SMv6 on the Super VLAN interface. Use the no or default form of this command is to restore the default setting.	
	ipv6 pim sparse-mode subvlan [all vid]	
	no ipv6 pim sparse-mode subvlan	
	default ipv6 pim sparse-mode subvlan	
Parameter	Parameter	Description
Description	all	Sends PIM packets to all sub VLANs.
	vid	Sends PIM packets to the specified VLAN.
Defaults	PIM-SMv6 is disabled on the Super VLAN interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	In general, a super VLAN includes many sub VLANs. If the PIM-SMv6 protocol is enabled on the interfaces of the super VLAN, PIM-SMv6 multicast packets will be replicated and sent to all sub VLANs. As a result, the traffic may exceed the device capability, causing protocol flapping. The Super VLAN interface is disabled with PIM-SMv6 generally. Use this command to enable PIM-SMv6 on the Super VLAN interface to send PIM packets to all sub VLANs or the specified sub VLAN.	
Configuration Examples	The following example enables PIM-SMv6 on the Super VLAN interface and sends PIM packets to sub VLAN 200. <pre>FS# configure terminal FS(config)# interface vlan 100 FS(config-if-vlan 100)# ipv6 pim sparse-mode subvlan 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.32 ipv6 pim spt-threshold

	Use this command to enable SPT switch.	
	Use the no or default form of this command to restore the default setting.	
	ipv6 pim spt-threshold [group-list ipv6_access-list]	
	no ipv6 pim spt-threshold [group-list ipv6_access-list]	
	default ipv6 pim spt-threshold [group-list ipv6_access-list]	

Parameter Description	Parameter	Description
	<i>ipv6_access_list</i>	(Optional) IPv6 ACL supporting named ACL
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable the RP tree-to-SPT tree switching function in a specific multicast group range (using group-list) or all multicast groups (not using group-list) .	
Configuration Examples	The following example enables the SPT switch. <pre>FS(config)# ipv6 pim spt-threshold acl FS(config)# ipv6 access-list acl FS(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad /128 ff66::6666/64</pre>	
Related Commands	Command	Description
	ipv6 access-list	N/A
Platform Description	N/A	

7.33 ipv6 pim ssm

	Use this command to enable SSM and set the SSM group address range. Use the no or default form of this command to restore the default setting.	
	ipv6 pim ssm { default range <i>ipv6_access-list</i> }	
	no ipv6 pim ssm	
	default ipv6 pim ssm	
Parameter Description	Parameter	Description
	default	Group in the range of FF3x::/32
	range <i>ipv6_access_list</i>	IPv6 ACL supporting named ACL
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable PIM-SSMv6 (or in some specific multicast groups).	

Configuration	The following example sets the source-specific multicast of the multicast group range ACL.	
Examples	FS# configure terminal	
	FS(config)# ipv6 pim ssm range aclFS(config-ipv6-acl)# permit ipv6 fe80::2d0:f8ff:fe22:33ad /128 ff32::3333/64	
Related Commands	Command	Description
	ipv6 access-list	N/A
Platform Description	N/A	

7.34 ipv6 pim static-rp-preferred

	Use this command to configure a higher priority for static RP over the C-RP. Use the no or default form of this command to restore the default setting.	
	ipv6 pim static-rp-preferred	
	no ipv6 pim static-rp-preferred	
	default ipv6 pim static-rp-preferred	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the priority of the RP elected through BSR mechanism is high than the one configured statically.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured, the priority of the static RP is higher than the one elected through the BSR mechanism.	
Configuration Examples	The following example configures the priority of the static RP is higher than the one elected through the BSR mechanism. FS(config-if)# ipv6 pim static-rp-preferred	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.35 ipv6 pim triggered-hello-delay

	Use this command to configure Triggered-Hello-Delay time on the interface.

	Use the no or default form of this command to restore the default setting.	
	ipv6 pim triggered-hello-delay <i>seconds</i>	
	no ipv6 pim triggered-hello-delay	
	default ipv6 pim triggered-hello-delay	
Parameter Description	Parameter	Description
	<i>seconds</i>	In the range from 1 to 5 in the unit of seconds.
Defaults	The default is 5 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to configure the triggered-hello-delay of the interface. When the interface starts or detects a new neighbor, it uses the trigger-hello-delay to generate random time, and then the interface sends the Hello message at the random time.	
Configuration Examples	The following example sets the triggered-hello-delay to 3 seconds. <pre>FS(config)# interface gi 0/3 FS(config-if-GigabitEthernet 0/3)# ipv6 pim triggered-hello-delay 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.36 show debugging

	Use this command to display the debugging status.	
	show debugging	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	

Configuration	The following example displays the debugging status.	
Examples	<pre>FS # show debugging PIM-SM Debugging status: PIM packet debugging is on.</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

7.37 show ipv6 pim sparse-mode bsr-router

	Use this command to display the BSR information.	
	show ipv6 pim sparse-mode bsr-router	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults		
Command Mode	Privileged EXEC mode/ global configuration mode / interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays BSR information. <pre>FS# show ipv6 pim sparse-mode bsr-router PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 3333::8888 Uptime:00:03:31, BSR Priority: 64, Hash mask length: 126 Next bootstrap message in 00:00:47 Role: Candidate BSR Priority: 64, Hash mask length: 126 State: Elected BSR Candidate RP: 3333::8888(GigabitEthernet 0/5) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:37</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.38 show ipv6 pim sparse-mode interface

	Use this command to display PIM-SMv6 interface information.	
	show ipv6 pim sparse-mode interface [<i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
	detail	(Optional) Displays the details of an interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the PIM-SMv6 interface information. <pre>FS #show ipv6 pim sparse-mode interface detail GigabitEthernet 0/5 (vif 1): Address fe80::2d0:f8ff:fe22:33ad, DR fe80::2d0:f8ff:fe22:34b3 Hello period 30 seconds, Next Hello in 6 seconds Triggered Hello period 5 seconds Secondary addresses: 3333::8888 4444::4444 Neighbors: fe80::2d0:f8ff:fe22:34b3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.39 show ipv6 pim sparse-mode local-members

	Use this command to display the local MLD information on the PIM-SMv6 interface.	
	show ipv6 pim sparse-mode local-members [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	(Optional) Interface name. This command takes effect for all interfaces by default.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the local MLD information on the PIM-SMv6 interface. <pre>FS (config-if)#show ipv6 pim sparse-mode local-members PIM Local membership information GigabitEthernet 0/5: (*, ff66::6666) : Include</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.40 show ipv6 pim sparse-mode mroute

	Use this command to display the PIM-SMv6 routing information.	
	show ipv6 pim sparse-mode mroute [<i>group-or-source-address</i> [<i>group-or-source-address</i>]]	
Parameter Description	Parameter	Description
	<i>group-or-source-address</i>	Group address or source address. Two addresses cannot both be the group addresses or the source addresses.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	This command is used to display route information. Only one group IPv6 address, one source IPv6 address or one	

	group IPv6 address-source IPv6 address pair can be configured at a time. You can also specify no group IP address or source IPv6 address.	
Configuration Examples	N/A	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.41 show ipv6 pim sparse-mode neighbor

	Use this command to display the neighbor information.	
	show ipv6 pim sparse-mode neighbor [detail]	
Parameter Description	Parameter	Description
	detail	(Optional) Displays the details of an interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide		
Configuration Examples	The following example displays the neighbor information.. <pre>FS# show ipv6 pim sparse-mode neighbor detail Nbr fe80::2d0:f8ff:fe22:34b3 (GigabitEthernet 0/5) Expires in 86 seconds Secondary addresses: 6666::6666</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.42 show ipv6 pim sparse-mode nexthop

	Use this command to display the next hop information, including the interface ID, address and metric.	
	show ipv6 pim sparse-mode nexthop	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	N/A	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.43 show ipv6 pim sparse-mode rp mapping

	Use this command to display the information on all RPs and the multicast groups they serve.	
	show ipv6 pim sparse-mode rp mapping	
Parameter Description	Parameter	Description
	mapping	All groups and RP information.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information on all RPs and the multicast groups they serve. FS# show ipv6 pim sparse-mode rp mapping	

	PIM Group-to-RP Mappings This system is the Bootstrap Router (v2) Group(s): ff00::/8 RP: 3333::1 Info source: 3333::1, via bootstrap, priority 192 Uptime: 00:12:40, expires: 00:01:50	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.44 show ipv6 pim sparse-mode rp-hash

	Use this command to display the RP information corresponding to the group address.	
	show ipv6 pim sparse-mode rp-hash <i>ipv6-group-address</i>	
Parameter Description	Parameter	Description
	<i>ipv6_group-address</i>	IPv6 group address
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the RP information corresponding to the group address.. FS# show ipv6 pim sparse-mode rp-hash ff66::6666 RP: 3333::8888 Info source: 3333::8888, via bootstrap PIMv2 Hash Value 126 RP 3333::8888, via bootstrap, priority 192, hash value 1468234650	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.45 show ipv6 pim sparse-mode track

	Use this command to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.																																																							
	show ipv6 pim sparse-mode track																																																							
Parameter Description	Parameter	Description																																																						
	N/A	N/A																																																						
Defaults	N/A																																																							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																																																							
Usage Guide	This command is used to display the number of sent and received PIM packets during the period from the beginning of the statistics till now.. When the system starts up, it sets the start time of the statistics. The start time of the statistics is reconfigured and the PIMv6 packet counter is cleared on calling the clear ipv6 pim sparse-mode track every time.																																																							
Configuration Examples	The following example displays the number of sent and received PIM packets during the period from the beginning of the statistics till now. <pre> FS# show ipv6 pim sparse-mode track PIMv6 packet counters track Elapsed time since counters cleared: 00:04:03 </pre> <table border="0"> <thead> <tr> <th></th> <th>received</th> <th>sent</th> </tr> </thead> <tbody> <tr> <td>Valid PIMSMv6 packets:</td> <td>0</td> <td>8</td> </tr> <tr> <td>Hello:</td> <td>0</td> <td>8</td> </tr> <tr> <td>Join-Prune:</td> <td>0</td> <td>0</td> </tr> <tr> <td>Register:</td> <td>0</td> <td>0</td> </tr> <tr> <td>Register-Stop:</td> <td>0</td> <td>0</td> </tr> <tr> <td>Assert:</td> <td>0</td> <td>0</td> </tr> <tr> <td>BSM:</td> <td>0</td> <td>0</td> </tr> <tr> <td>C-RP-ADV:</td> <td>0</td> <td>0</td> </tr> <tr> <td>PIMDMv6-Graft:</td> <td>0</td> <td></td> </tr> <tr> <td>PIMDMv6-Graft-Ack:</td> <td>0</td> <td></td> </tr> <tr> <td>PIMDMv6-State-Refresh:</td> <td>0</td> <td></td> </tr> <tr> <td>Unknown PIMv6 Type:</td> <td>0</td> <td></td> </tr> <tr> <td>Errors:</td> <td></td> <td></td> </tr> <tr> <td>Malformed packets:</td> <td></td> <td>0</td> </tr> <tr> <td>Bad checksums:</td> <td></td> <td>0</td> </tr> <tr> <td>Send errors:</td> <td></td> <td>0</td> </tr> <tr> <td>Packets received with unknown PIMv6 version:</td> <td>0</td> <td></td> </tr> </tbody> </table>			received	sent	Valid PIMSMv6 packets:	0	8	Hello:	0	8	Join-Prune:	0	0	Register:	0	0	Register-Stop:	0	0	Assert:	0	0	BSM:	0	0	C-RP-ADV:	0	0	PIMDMv6-Graft:	0		PIMDMv6-Graft-Ack:	0		PIMDMv6-State-Refresh:	0		Unknown PIMv6 Type:	0		Errors:			Malformed packets:		0	Bad checksums:		0	Send errors:		0	Packets received with unknown PIMv6 version:	0	
	received	sent																																																						
Valid PIMSMv6 packets:	0	8																																																						
Hello:	0	8																																																						
Join-Prune:	0	0																																																						
Register:	0	0																																																						
Register-Stop:	0	0																																																						
Assert:	0	0																																																						
BSM:	0	0																																																						
C-RP-ADV:	0	0																																																						
PIMDMv6-Graft:	0																																																							
PIMDMv6-Graft-Ack:	0																																																							
PIMDMv6-State-Refresh:	0																																																							
Unknown PIMv6 Type:	0																																																							
Errors:																																																								
Malformed packets:		0																																																						
Bad checksums:		0																																																						
Send errors:		0																																																						
Packets received with unknown PIMv6 version:	0																																																							

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8 IGMP Snooping Commands

8.1 clear ip igmp snooping gda-table

	Use this command to clear the Group Destination Address (GDA) table. clear ip igmp snooping gda-table	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID, and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the clear ip igmp snooping gda-table command.	
Configuration Examples	The following example clears the Group Destination Address (GDA) table. FS# clear ip igmp snooping gda-table	
Platform Description	N/A	

8.2 clear ip igmp snooping statistics

	Use this command to clear IGMP Snooping statistics. clear ip igmp snooping statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the IGMP Snooping statistics, which can be displayed by using the show ip igmp snooping statistics command.	

Configuration	The following example clears the IGMP Snooping statistics.
Examples	FS# clear ip igmp snooping statistics
Platform	N/A
Description	

8.3 deny

	Use this command to deny the forwarding of the multicast streams in the range specified by the profile. deny	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The forwarding of the multicast streams in the range specified by the profile is denied.	
Command Mode	Profile configuration mode	
Usage Guide	First, configure the multicast range using the range command in the profile configuration mode. In addition, the profile must be applied to the interface in order to make the profile configuration take effect.	
Configuration Examples	The following is an example of deny the forwarding of the multicast stream 224.2.2.2 to 224.2.2.244. FS(config)# ip igmp profile 1 FS(config-profile)# range 224.2.2.2 224.2.2.244 FS(config-profile)# deny	
Platform Description	N/A	

8.4 ip igmp profile

	Use this command to create a profile and enter the IGMP profile configuration mode. Use the no or default form of this command to restore the default setting. ip igmp profile <i>profile-number</i> no ip igmp profile <i>profile-number</i> default ip igmp profile <i>profile-number</i>	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number, in the range from 1 to 1024
Defaults	No profile is created by default.	

Command Mode	Global configuration mode
Usage Guide	The profile is a filter to permit/deny specified groups in the following steps: ● Use the ip igmp profile command to create a profile and enter profile configuration mode. ● Use the range command to define a profile range. ● Use the permit command to permit this profile in the filtering, or use the deny command to deny this profile in the filtering. ● If the deny command is used without any profile specified, all profiles in the profile are permitted. ● If the permit command is used without any profile specified, all profiles in the profile are denied.
Configuration Examples	The following example creates and permits profile 1 with addresses from 224.2.2.2 to 224.2.2.244. <pre>FS(config)# ip igmp profile 1 FS(config-profile)# range 224.2.2.2 224.2.2.244 FS(config-profile)# permit</pre>
Platform Description	N/A

8.5 ip igmp snooping

	Use this command to enable IGMP snooping and enter the IVGL mode.	
	ip igmp snooping ivgl Use this command to enable IGMP snooping and enter the SVGL mode. ip igmp snooping svgl Use this command to enable IGMP snooping and enter the IVGL-SVGL mode. ip igmp snooping ivgl-svgl Use the no or default command to restore the default setting. no ip igmp snooping default ip igmp snooping	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	IGMP Snooping is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	● IVGL (Independent VLAN Group Learning): In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN. ● SVGL (Shared VLAN Group Learning): In this mode, the hosts in different VLANs share the same multicast	

	flow. A host can request multicast flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3: ● IVGL-SVGL mode: also known as promiscuous mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN. ● For wireless products, only IVGL mode is supported. Use the ip igmp snooping command to enable IGMP Snooping in global configuration mode, and use the igmp snooping command in AP configuration mode.  SVGL mode and IVGL-SVGL mode conflict with the IP multicast function.  PIM Snooping must depend on either IVGL or IVGL-SVGL mode of IGMP Snooping. Use no ip igmp snooping command to disable IGMP Snooping after PIM Snooping is disabled.
Configuration Examples	The following example enables IGMP Snooping and enters the IVGL mode. <pre>FS(config)# ip igmp snooping ivgl</pre> The following example enables IGMP Snooping and enters the SVGL mode. <pre>FS(config)# ip igmp snooping svgl FS(config)# ip igmp snooping svgl profile 1</pre> The following example enables IGMP Snooping and enters the IVGL-SVGL mode. <pre>FS(config)# ip igmp snooping ivgl-svgl FS(config)# ip igmp snooping svgl profile 1</pre> The following example enables IGMP Snooping on APs. <pre>FS(config)# ip igmp snooping FS(ap-config)# igmp snooping</pre>
Platform Description	N/A

8.6 ip igmp snooping dyn-mr-aging-time

	Use this command to set the aging time of a dynamic routing interface. Use the no or default form of this command to restore the default setting.
	ip igmp snooping dyn-mr-aging-time <i>seconds</i> no ip igmp snooping dyn-mr-aging-time default ip igmp snooping dyn-mr-aging-time

Parameter Description	Parameter	Description
	<i>seconds</i>	Aging time from 1 to 3,600 in the unit of seconds
Defaults	The default is 300 seconds.	
Command Mode	Global configuration mode	
Usage Guide	If a dynamic routing interface does not receive IGMP query packets or PIM hello packets before aged, this interface will be deleted. When the dynamic routing interface learning function is enabled, this command sets the aging time of the routing interface. If the aging time is set too short, the routes may be added and deleted frequently.	
Configuration Examples	The following example sets the aging time of the routing interface that the switch learns dynamically to 100 seconds. <pre>FS(config)# ip igmp snooping dyn-mr-aging-time 100</pre>	
Platform Description	N/A	

8.7 ip igmp snooping fast-leave enable

	Use this command to enable the fast leave function. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping fast-leave enable no ip igmp snooping fast-leave enable default ip igmp snooping fast-leave enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After you execute this command to enable the fast-leave function, the system will remove the corresponding multicast group on the corresponding interface upon the receipt of the IGMP leave message. Subsequently, when the system receives a specific group query packet, the system does not forward it to the corresponding interface. Leave packets refer to the IGMPv2 leave packets. The fast leave function applies to scenarios in which one interface is connected to only one host. This function saves bandwidth and resources.	
Configuration	The following example enables the fast leave function.	

Examples	FS(config)# ip igmp snooping fast-leave
Platform	N/A
Description	

8.8 ip igmp snooping filter

	Use this command to specify the profile for ports. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping filter <i>profile-number</i> no ip igmp snooping filter <i>profile-number</i> default ip igmp snooping filter	
	Use this command to specify the profile for VLANs. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping vlan <i>vlan-id</i> filter <i>profile-number</i> no ip igmp snooping vlan <i>vlan-id</i> filter default ip igmp snooping vlan <i>vlan-id</i> filter	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number from 1 to 1024
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode/Interface configuration mode	
Usage Guide	A specific profile must be created before association.	
Configuration Examples	The following example specifies profile 1 for interface fastEthernet 0/1. FS(config)# interface fastEthernet 0/1 FS(config-if)# ip igmp snooping filter 1	
Platform	N/A	
Description		

8.9 ip igmp snooping host-aging-time

	Use this command to configure the aging time of IGMP dynamic ports. Use the no or default form of this command to restore the default setting.
	ip igmp snooping host-aging-time <i>seconds</i>
	no ip igmp snooping host-aging-time
	default ip igmp snooping host-aging-time

Parameter	Parameter	Description
Description	<i>seconds</i>	Aging time. The unit is second. The value ranges from 1 to 65,535.
Defaults	The default is 260 seconds.	
Command Mode	Global configuration mode	
Usage Guide	The aging time of a dynamic port is set by the system when the port receives an IGMP packet from the host for joining a certain IP multicast group. When such an IGMP packet is received, the system resets the aging timer for the port. The duration of this timer is determined by host-aging-time. If the timer expires, the system determines that there is no host in this port for receiving multicast packets. The multicast device removes the port from the IGMP Snooping group. After the ip igmp snooping host-aging-time command is executed, the aging time will be determined by host-aging-time. This command takes effect only after the system receives the next IGMP packet. This command does not change the current aging time.	
Configuration Examples	The following example sets the aging time to 30 seconds. <pre>FS(config)# ip igmp snooping host-aging-time 30</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.10 ip igmp snooping l2-entry-limit

	Use this command to set the maximum number of multicast groups. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping l2-entry-limit <i>number</i>	
	no ip igmp snooping l2-entry-limit default ip igmp snooping l2-entry-limit	
Parameter Description	Parameter	Description
	<i>number</i>	Number of multicast groups. The value ranges from 0 to 65,536.
Defaults	The default is 65,536.	
Command Mode	Global configuration mode	
Usage Guide	The maximum number of multicast groups includes the multicast groups in all ports of all VLANs (including dynamic and static multicast groups). When the number of multicast groups reaches the limit, learning new group records and configuring new static multicast group ports are not allowed.	

Configuration Examples	The following example sets the maximum number of multicast groups to 2000.	
	FS(config)# ip igmp snooping l2-entry-limit 2000	
Related Commands	Command	Description
	show ip igmp snooping	Displays the maximum number of multicast groups.
Platform Description	N/A	

8.11 ip igmp snooping limit-ipmc

	Use this command to add a multicast source IP address check entry. Use the no or default form of this command is used to delete a source IP checklist entry.	
	ip igmp snooping limit-ipmc vlan <i>vid</i> address <i>gaddress</i> server <i>saddress</i> no ip igmp snooping limit-ipmc vlan <i>vid</i> address <i>gaddress</i> default ip igmp snooping limit-ipmc vlan <i>vid</i> address <i>gaddress</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID
	<i>group-address</i>	Multicast group address
	<i>source-address</i>	Multicast source IP address
Defaults	Only source IP address check is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to filter the multicast packets. With it enabled, all multicast packets from illegal IP addresses will be discarded.  Source IP address check and multicast routing function cannot be enabled meanwhile. Configuration steps: 1. Enable source IP address check and specify the source IP address. 2. (Optional) Specify the multicast group address and source IP address for a specific VLAN.	
Configuration Examples	The following example enables source address check to receive multicast packets only from 192.168.1.10 and allows packets into VLAN 203 and VLAN 104 from (192.168.1.10 , 229.1.1.1). <pre>FS# configure terminal FS(config)# ip igmp snooping source-check default-server 192.168.1.10 FS(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server 192.168.1.10 FS(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server 192.168.1.10 FS(config)# end</pre>	
Platform Description	N/A	

8.12 ip igmp snooping max-groups

	Use this command to configure the maximum number of groups that can be added dynamically to this interface. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping max-groups <i>number</i> no ip igmp snooping max-groups default ip igmp snooping max-groups	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum group number from 0 to 1,024
Defaults	No maximum group number is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	If a maximum number of multicast groups are configured, the device will no longer receive and process IGMP Report messages when the number of multicast groups on this interface is beyond the range.	
Configuration Examples	The following example configures the maximum number of multicast groups to 100 on the megabit interface 0/1: <pre>FS(config)# interface Ethernet 0/1 FS(config-if)# ip igmp snooping max-group 100</pre>	
Platform Description	N/A	

8.13 ip igmp snooping mrouter learn pim-dvmrp

	Use this command to configure a device to listen to the IGMP Query/Dvmrp or PIM Help packets dynamically in order to automatically identify a routing interface Use the no form of this command to disable the dynamic learning. Use the default form of this command to restore the default setting. ip igmp snooping [vlan vid] mrouter learn pim-dvmrp no ip igmp snooping [vlan vid] mrouter learn pim-dvmrp default ip igmp snooping [vlan vid] mrouter learn pim-dvmrp	
Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	This function is enabled by default.	
Command	Global configuration mode	

Mode	
Usage Guide	Routing interface is a port through which a multicast device (with IGMP Snooping enabled) is directly connected to a multicast neighbouring device (with multicast routing protocols enabled). By default, the dynamic routing interface learning function is enabled. You can use the no form of this command to disable this function and clear all routing interfaces learnt dynamically. With dynamic routing interface learning function disabled globally, the function of all vlans will be disabled. Beside, with this function enabled globally, if the function of specified vlan is disabled, the dynamic routing interface learning function of the corresponding vlan is disabled. When the source port check function is enabled, only the multicast flow enters from the routing interface is legal and it is forwarded to the registered interface by the multicast equipment, the multicast flow from the non routing interface is considered to be the illegal and is discarded. With the source port check function enabled, the dynamic routing interface learning function will improve the application flexibility of IGMP snooping.
Configuration Examples	The following example enables the dynamic routing interface learning function on VLAN 1. <pre>FS(config)# no ip igmp snooping mrouter learn pim-dvmrp FS(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp</pre>
Platform Description	N/A

8.14 ip igmp snooping preview

	Use this command to allow the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use no or default form of this command to disable multicast preview.	
	ip igmp snooping preview <i>profile-number</i> no ip igmp snooping preview default ip igmp snooping preview	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number (1-1024)
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Apply the IGMP Profile to a multicast preview function. When the user doesn't have access to the multicast streams (namely the user might be filtered by IGMP Snooping filter), it can allow the user to preview partial contents. This function shall be used in conjunction with IGMP Snooping filter or multicast control in order to realize effective multicast preview.	
Configuration	The following example associates the profile 2 to the Ethernet 0/1 and associates multicast preview with profile 1.	

Examples	<pre>FS(config)# ip igmp snooping preview 1 FS(config-if)# int Ethernet 0/1 FS(config-if)# ip igmp snooping filter 2</pre>
Platform	N/A
Description	

8.15 ip igmp snooping preview interval

	Use this command to configure the interval that allows the user to preview the specific multicast streams when the user doesn't have access to such multicast streams. Use no or default form of this command to restore the default setting.	
	ip igmp snooping preview interval <i>seconds</i> no ip igmp snooping preview interval default ip igmp snooping preview interval	
Parameter		
Description	Parameter	Description
	<i>seconds</i>	Preview interval from 1 to 300 in the unit of seconds
Defaults	The default is 60 seconds.	
Command	Global configuration mode	
Mode		
Usage Guide	N/A	
Configuration	The following example sets the multicast preview interval as 100 seconds on the 100M port of 0/1:	
Examples	<pre>FS(config)# ip igmp snooping preview 1 FS(config)# ip igmp snooping preview interval 100</pre>	
Platform	N/A	
Description		

8.16 ip igmp snooping querier

	Use this command to enable the IGMP querier. Use no or default form of this command to restore the default setting.	
	ip igmp snooping [vlan vid] querier no ip igmp snooping [vlan vid] querier default ip igmp snooping [vlan vid] querier	
Parameter		
Description	Parameter	Description
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	After globally enabling the IGMP querier, you must enable the IGMP querier function in VLAN to activate this function. If the IGMP querier function is disabled globally, the IGMP querier will be disabled in all VLANs.
Configuration Examples	The following example enables the IGMP querier function in VLAN 2. <pre>FS(config)# ip igmp snooping querier FS(config)# ip igmp snooping vlan 2 querier</pre>
Platform Description	N/A

8.17 ip igmp snooping querier address

	Use this command to specify a source IP address for IGMP querier. Use no or default form of this command to remove the source IP address configured.	
	ip igmp snooping [vlan vid] querier address a.b.c.d no ip igmp snooping [vlan vid] querier address default ip igmp snooping [vlan vid] querier address	
Parameter Description	Parameter	Description
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
	a.b.c.d	Source IP address of the IGMP querier
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	After enabling IGMP querier, you must configure a source IP address for the IGMP querier to activate this function.. If the IGMP querier source IP has been specified in VLAN, the source IP configured in the relevant VLAN will be used first.	
Configuration Examples	The following example specifies the source IP of the IGMP querier as 1.1.1.1 on the device. <pre>FS(config)# ip igmp snooping querier address 1.1.1.1</pre> The following example specifies the source IP of the IGMP querier as 1.1.1.1 in VLAN 3. <pre>FS(config)# ip igmp snooping vlan 3 querier address 1.1.1.1</pre>	
Platform Description		

8.18 ip igmp snooping querier max-response-time

	Use this command to configure the maximum response time of the IGMP querier. Use no or default form of this command to restore to the default setting.	
	ip igmp snooping [vlan vid] querier max-response-time seconds no ip igmp snooping [vlan vid] querier max-response-time default ip igmp snooping [vlan vid] querier max-response-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	Maximum response time from 1 to 25 in the unit of seconds
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	The default is 10 seconds.	
Command Mode	Global configuration mode	
Usage Guide	By default, the maximum response time is 10 seconds. If the maximum response time has been specified in the corresponding VLAN, the value specified in VLAN will be used first.	
Configuration Examples	The following example specifies the maximum response time of the IGMP querier on the device. <pre>FS(config)# ip igmp snooping querier max-response-time 15</pre> The following example specifies the maximum response time of the IGMP querier in VLAN 3. <pre>FS(config)# ip igmp snooping vlan 3 querier max-response-time 15</pre>	
Platform Description	N/A	

8.19 ip igmp snooping querier query-interval

	Use this command to specify the interval for IGMP querier to send query packets. Use no or default form of this command to restore the default setting.	
	ip igmp snooping [vlan vid] querier query-interval seconds no ip igmp snooping [vlan vid] querier query-interval default ip igmp snooping [vlan vid] querier query-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Query interval from 1 to 18,000 in the unit of seconds
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	The default is 60 seconds.	

Command Mode	Global configuration mode
Usage Guide	If the query interval has been configured in the corresponding VLAN, the value specified in VLAN will be used first.
Configuration Examples	The following example configures the query interval on the device. <pre>FS(config)# ip igmp snooping querier query-interval 100</pre> The following example configures the query interval in VLAN 3. <pre>FS(config)# ip igmp snooping vlan 3 querier query-interval 100</pre>
Platform Description	N/A

8.20 ip igmp snooping querier timer expiry

	Use this command to specify the expiration timer for non-querier. Use no form of this command to restore the default setting.	
	<pre>ip igmp snooping [vlan vid] querier timer expiry seconds</pre> <pre>ip igmp snooping [vlan vid] querier timer expiry seconds</pre> <pre>default ip igmp snooping [vlan vid] querier timer expiry</pre>	
Parameter Description	Parameter	Description
	<i>seconds</i>	The expiration timer from 60 to 300 in the unit of seconds
	<i>vlan vid</i>	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	The default is 125 seconds.	
Command Mode	Global configuration mode	
Usage Guide	After globally enabling IGMP querier, if the device is elected as a non-querier, execute this command to change the expiration timer for non-querier. If expiration timer has been configured in the corresponding VLAN, the value specified in VLAN will be used first.	
Configuration Examples	The following example configures the non-querier expiration timer on the device. <pre>FS(config)# ip igmp snooping querier timer expiry 60</pre> The following example configures the non-querier expiration timer in VLAN 3. <pre>FS(config)# ip igmp snooping vlan 3 querier timer expiry 60</pre>	
Platform Description	N/A	

8.21 ip igmp snooping querier version

	Use the following commands to specify IGMP Snooping querier version. ip igmp snooping [vlan vid] querier version 1 ip igmp snooping [vlan vid] querier version 2 ip igmp snooping [vlan vid] querier version 3	
	Use no or default form of this command to restore to the default setting. no ip igmp snooping [vlan vid] querier version default ip igmp snooping [vlan vid] querier version	
Parameter Description	Parameter	Description
	vlan vid	VLAN ID. By default, the specified version is supported on all VLANs.
Defaults	The default version is IGMPv2.	
Command Mode	Global configuration mode	
Usage Guide	If an IGMP querier version has been configured in a VLAN, the version specified in the VLAN will be used first.	
Configuration Examples	The following example configures IGMP querier version on the device. FS(config)# ip igmp snooping querier version 1	
Platform Description	N/A	

8.22 ip igmp snooping query-max-response-time

	Use this command to specify the time for the switch to wait for the member join message after receiving the query message. Use the no or default form of this command to restore the default setting. ip igmp snooping query-max-response-time seconds no ip igmp snooping query-max-resposne-time default ip igmp snooping query-max-response-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	The aging time of the routing interface that the switch learns dynamically, in the range from 1 to 65.535
Defaults	The default is 10 seconds.	
Command	Global configuration mode	

Mode	
Usage Guide	You can specify the time for the switch to wait for the member join message after receiving the query message. If the switch does not receive the member join message in the specified time, it considers that the member has left and then deletes the member. This command lets you adjust the waiting time after receiving the query message. This command takes effect only after the switch receives the next member join message. This command does not change the current wait time.
Configuration Examples	The following examples sets the aging time of the routing interface that the switch learns dynamically to 100 seconds. <pre>FS(config)# ip igmp snooping query-max-response-time 100</pre>
Platform Description	N/A

8.23 ip igmp snooping source-check default-server

	Use this command to enable the source IP address check to permit one or several IPMC flows from the server of the specified IP address. Use the no or default form of this command is used to restore the default setting.	
	<pre>ip igmp snooping source-check default-server source-address no ip igmp snooping source-check default ip igmp snooping source-check</pre>	
Parameter Description	Parameter	Description
	<i>source-address</i>	Default multicast source IP address
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The source IP address check function takes effect globally. Once it is enabled, only the IPMC streams from the specified IP address are permitted.  Source IP address check and IP multicast function cannot work meanwhile. The device allows users to configure the source IP address of all IPMC streams, called default multicast server. The default server must be set as long as the source IP address check function is enabled.	
Configuration Examples	The following example enables the multicast source IP address check function. <pre>FS# configure terminal FS(config)# ip igmp snooping source-check default-server 192.168.1.10</pre>	

	<pre>FS(config)# ip igmp snooping limit-ipmc vlan 203 address 229.1.1.1 server 192.168.1.10 FS(config)# ip igmp snooping limit-ipmc vlan 204 address 229.1.1.1 server 192.168.1.10 FS(config)# end</pre>
Platform	N/A
Description	

8.24 ip igmp snooping source-check port

	Use this command to enable the source port check function of IGMP Snooping. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping source-check port no ip igmp snooping source-check port default ip igmp snooping source-check port	
Parameter	Parameter	Description
Description		
	N/A	N/A
Defaults	This function is disabled by default.	
Command	Global configuration mode	
Mode		
Usage Guide	The source port check function is used to permit one or several IPMC flows from the mroute port. When it is enabled, only the IPMC streams from the specified port are permitted. When it is disabled, all the IPMC streams are permitted and forwarded.	
Configuration	The following example enables the source port check function of IGMP Snooping.	
Examples	<pre>FS(config)# ip igmp snooping source-check port</pre>	
Platform	N/A	
Description		

8.25 ip igmp snooping suppression enable

	Use this command to enable IGMP snooping suppression. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping suppression enable no ip igmp snooping suppression enable default ip igmp snooping suppression enable	
Parameter	Parameter	Description
Description		
	N/A	N/A

Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	When this function is enabled, IGMP Snooping only forwards the first report from a specific VLAN or group, and suppresses the following reports to constrain traffic in the networks. This function is only supported on IGMPv1 and IGMPv2 reports.
Configuration Examples	The following example enables IGMP snooping suppression on the device. FS(config)# ip igmp snooping suppression enable
Platform Description	N/A

8.26 ip igmp snooping svgl profile

	Use this command to specify the multicast group address range applied in the SVGL/IVGL-SVGL mode. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping svgl profile <i>profile-number</i> no ip igmp snooping svgl profile default ip igmp snooping svgl profile	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number, in the range of 1-1,024
Defaults	No profile is associated.	
Command Mode	Global configuration mode	
Usage Guide	When the IGMP Snooping works in the SVGL and IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across the VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN.	
Configuration Examples	The following example specifies the profile 2 applied in SVGL mode. FS(config)# ip igmp snooping svgl profile 2	
Platform Description	N/A	

8.27 ip igmp snooping svgl subvlan

	Use this command to specify the subvlan of multicast VLAN. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping svgl subvlan <i>[vid-range]</i> no ip igmp snooping svgl subvlan <i>[vid-range]</i> default ip igmp snooping svgl subvlan <i>[vid-range]</i>	
Parameter Description	Parameter	Description
	<i>vid-range</i>	VLAN ID or range of VLAN ID
Defaults	By default, all VLANs except shared VLANs serve as its sub VLANs.	
Command Mode	Global configuration mode	
Usage Guide	This command only takes effect in SVGL and IVGL-SVGL mode.	
Configuration Examples	The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs. FS(config)# ip igmp snooping svgl vlan 3 FS(config)# ip igmp snooping svgl subvlan 2,5-7	
Platform Description	N/A	

8.28 ip igmp snooping svgl vlan

	Use this command to specify the shared VLAN in SVGL mode. Use the no form of this command to restore the default setting.	
	ip igmp snooping svgl vlan <i>vid</i> no ip igmp snooping svgl vlan default ip igmp snooping svgl vlan	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID
Defaults	By default , the shared VLAN is VLAN 1.	
Command Mode	Global configuration mode	
Usage Guide	This command only works in the SVGL and IVGL-SVGL mode.	

Configuration	The following example specifies VLAN 3 as the shared VLAN and VLAN 2, VLAN 5 to 7 as the sub VLANs.
Examples	<pre>FS(config)# ip igmp snooping svgi vlan 3 FS(config)# ip igmp snooping svgi subvlan 2,5-7</pre>
Platform	N/A
Description	

8.29 ip igmp snooping tunnel

	Use this command to enable 802.1Q tunneling (QinQ) support for IGMP Snooping. Use the no or default form of this command to restore the default setting.	
	ip igmp snooping tunnel no ip igmp snooping tunnel default ip igmp snooping tunnel	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled.	
Command Mode	Global configuration mode	
Usage Guide	After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways: ● First: QinQ transmits IGMP packets transparently. Create multicast entries in the VLAN to which the IGMP packets belong, and forward IGMP packets in the VLAN. ● For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of Port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed by Port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10. ● Second: Create multicast entries in the default VLAN to which the dot1q-tunnel ports belong, and forward multicast packets in the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port. ● For example: It is assumed that IGMP Snooping has been enabled on the device; Port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 are allowed Port A. When multicast requests of VLAN 10 are sent to Port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1. By default, the second way is used.	
Configuration	The following example enables QinQ support for IGMP Snooping.	

Examples	FS(config)# ip igmp snooping tunnel
Platform	N/A
Description	

8.30 ip igmp snooping vlan

	Use this command to enable the IGMP Snooping in the specified VLAN and enter IVGL mode. Use the no form of this command is used to disable the IGMP Snooping. Use the default form of this command to restore the default setting.	
	ip igmp snooping vlan <i>vid</i> no ip igmp snooping vlan <i>vid</i> default ip igmp snooping vlan <i>vid</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
Defaults	IGMP Snooping is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable or disable the IGMP snooping on the specified vlan.  The PIM Snooping in the specified VLAN works only when IGMP Snooping is configured. To disable PIM Snooping, you must disable IGMP Snooping in the VLAN first, or disabling will fail and be prompted.	
Configuration Examples	The following example enters IVGL mode and disables the IGMP Snooping in the VLAN 2. <pre>FS(config)# ip igmp snooping ivgl FS(config)# no ip igmp snooping vlan 2</pre>	
Platform	N/A	
Description		

8.31 ip igmp snooping vlan mrouter interface

	Use this command to configure a static routing interface. Use the no form of this command to delete a static routing interface. Use the default form of this command to restore the default setting.	
	ip igmp snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i> no ip igmp snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i> default ip igmp snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>	

Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
	<i>interface-type interface-number</i>	Interface ID
Defaults	No static routing interface is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	A dynamic routing interface is learned dynamically through IGMP Snooping. A static routing interface is configured by using this command and cannot age. When an interface is configured as a static routing interface, all multicast streams received on this interface will be forwarded. When the source port check function is enabled, only the multicast flows from the routing interface are forwarded, and other flows will be discarded.	
Configuration Examples	The following example configures a static routing interface. <pre>FS(config)# ip igmp snooping vlan 1 mrout erinterface fastEthernet 0/1</pre>	
Platform Description	N/A	

8.32 ip igmp snooping vlan static interface

	Use this command to configure a static member interface of a multicast group. Use the no form of this command to delete a static member interface from a multicast group. Use the default form of this command to restore the default setting.	
	ip igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i> no ip igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i> default ip igmp snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID in the range from 1 to 4,094
	<i>ip-addr</i>	Multicast IP address
	<i>interface-id</i>	Interface ID
Defaults	No static member interface of any multicast group is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	The IGMP Snooping GDA table contains VLAN IDs (VIDs), group addresses, routing interface (static or dynamic) ID,	

	and member interface ID. Among them, the VID and group address identify a forwarding entry; the static routing interfaces will not age and cannot be deleted by using the clear ip igmp snooping gda-table command.
Configuration Examples	The following example configures a static member interface for the multicast group 224.1.1.1. FS(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/1
Platform Description	N/A

8.33 permit

	Use this command to permit the multicast forwarding for specified ranges of a specified profile.	
	permit	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The forwarding of the multicast streams in the range specified by the profile is denied.	
Command Mode	Profile configuration mode	
Usage Guide	A profile is used to filter a group of multicast packets, so as to assist other features. Configuration steps: 1. Use the ip igmp profile command to create a profile and enter profile configuration mode. 2. Use the range command to define a range for the profile. 3. Use the permit command to permit the multicast forwarding for the profile.	
Configuration Examples	The following example permits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244 of profile 1. <pre>FS(config)# ip igmp profile 1 FS(config-profile)# range 224.2.2.2 224.2.2.244 FS(config-profile)# permit</pre>	
Platform Description	N/A	

8.34 range

	Use this command to define a range for a specific profile. Use the no form of the command to remove the range from the profile.
	range <i>low-ip-address</i> [<i>high-ip-address</i>] no range <i>low-ip-address</i> [<i>high-ip-address</i>]

Parameter Description	Parameter	Description
	<i>low-ip-address</i>	Start address of a range
	<i>high-ip-address</i>	End address of a range
Defaults	No range is defined for a profile by default.	
Command Mode	Profile configuration mode	
Usage Guide	A profile is used to filter a group of multicast packets, so as to assist other features. Configuration steps: 1. Use the ip igmp profile command to create a profile and enter profile configuration mode. 2. Use the range command to define a range for the profile. 3. Use the permit command to permit the multicast forwarding for the profile.	
Configuration Examples	The following is an example of allowingpermits the forwarding of the multicast streams from 224.2.2.2 to 224.2.2.244: of profile 1. <pre>FS(config)# ip igmp profile 1 FS(config-profile)# range 224.2.2.2 224.2.2.244224.2.2 FS(config-profile)# permit</pre>	
Platform Description	N/A	

8.35 show ip igmp profile

	Use this command to display the profile information.	
	show ip igmp profile <i>profile-number</i>	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Displays configuration information of the designated profile.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to display the profile information.	
Configuration Examples	The following example displays the profile information. <pre>FS(config-if)# show ip igmp profile Profile 1</pre>	

Permit
range 224.0.1.0, 239.255.255.255

8.36 show ip igmp snooping

	Use this command to display related information of IGMP Snooping.	
	show ip igmp snooping [gda-table interfaces <i>interface-type interface-number</i> mdevice statistics [vlan <i>vlan-id</i>] querier [detail vlan <i>vid</i>] user-info]	
Parameter Description	Parameter	Description
	vlan <i>vid</i>	VLAN ID. By default, IGMP Snooping information of all VLANs are displayed.
	<i>interface-type interface-number</i>	Interface type and number
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays global IGMP Snooping information. <pre>FS#show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2 IGMP Snooping version: 2IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)</pre> The following example displays VLAN1 IGMP Snooping information. <pre>FS#show ip igmp snooping vlan 1 IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Global IGMPv2 Fast-Leave :Disable Global multicast router learning mode :Enable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time : 300(Seconds)</pre>	

	Dynamic Host Aging Time : 260(Seconds) vlan 1 ----- IGMP Snooping state: Enable Multicast router learning mode: pim-dvmrp IGMP Fast-Leave: Disable IGMP VLAN querier: Disable IGMP VLAN Mode: STATIC
Platform	N/A
Description	

9 MLD Snooping Commands

9.1 clear ipv6 mld snooping gda-table

	Use this command to clear the forwarding table information learned dynamically.	
	clear ipv6 mld snooping gda-table	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the forwarding table information learned dynamically.	
Configuration Examples	The following example clears the forwarding table information learned dynamically: FS# clear ipv6 mld snooping gda-table	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.2 clear ipv6 mld snooping statistics

	Use this command to clear the MLD Snooping statistics, including the entry number, the entry volume, the number of various received packets, the group information and the interface information of the corresponding group.	
	clear ipv6 mld snooping statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	Use the show ipv6 mld snooping statistics command to verify the configuration.	
Configuration Examples	The following example clears the MLD Snooping statistics.	
	FS# clear ipv6 mld snooping statistics	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.3 deny

	Use this command to prevent the multicast flow profile within the specified range from being forwarded in the profile configuration mode.	
	deny	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default profile action is deny .	
Command Mode	Profile configuration mode	
Usage Guide	Profile is a kind of group “filter” that can be referred to by other functions. Configuration Steps: 1. Use the ipv6mld profile command to create a profile and enter the profile mode. 2. Use the range command to define a group. 3. Use the permit command to allow this group to pass the filtering; Use the deny command to filter the packets of this group. The default command is deny.	
Configuration Examples	The following example prevents the multicast flow profile within the range from FF15::1 to FF15::100 from being forwarded. <pre>FS(config)# ipv6 mld profile 1 FS(config-profile)# range FF15::1 FF15::100 FS(config-profile)# deny</pre>	
Related Commands	Command	Description
	ipv6 mld profile	Creates one profile.

	range	Sets the multicast address range.
	permit	Sets the profile action permit.
Platform Description	N/A	

9.4 ipv6 mld profile

	Use the following command to create a profile. Use the no or default form of this command to delete a profile.	
	ipv6 mld profile <i>profile-number</i>	
	no ipv6 mld profile <i>profile-number</i>	
	default ipv6 mld profile <i>profile-number</i>	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number, in the range from 1 to 1024.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Profile is a kind of group “filter” that can be referred to by other functions. Configuration Steps: 1. Use the ipv6mld profile command to create a profile and enter the profile mode. 2. Use the range command to define a group. 3. Use the permit command to allow this group to pass the filtering; Use the deny command to filter the packets of this group. The default command is deny.	
Configuration Examples	The following example creates profile 1 and allows the packets sent by devices with MAC address ranging from FF15::1 to FF15::100 to pass the filtering. <pre>FS(config)#ipv6 mld profile 1 FS(config-profile)#range FF15::1 FF15::100 FS(config-profile)#permit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.5 ipv6 mld snooping

	Use this command to enable MLD Snooping and specify IVGL/SVGL/IVGL-SVGL mode. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping {ivgl svgl ivgl-svgl}	
	no ipv6 mld snooping {ivgl svgl ivgl-svgl}	
	default ipv6 mld snooping {ivgl svgl ivgl-svgl}	
Parameter Description	Parameter	Description
	ivgl	MLD Snooping is running IVGL mode.
	svgl	MLD Snooping is running SVGL mode.
	ivgl-svgl	MLD Snooping is running IVGL-SVGL mode.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	● In IVGL mode, multicast flow in each VLAN is independent. The host only requests multicast flow from the routing interface within the same VLAN. The device forwards the multicast flow from any VLAN to the member port within the same VLAN. ● In SVGL mode, multicast flow is shared among VLANs. The host can request multicast flow across VLANs. Shared VLAN (VLAN 1 by default) should be specified. Only multicast flow from Shared VLAN can be forwarded to all member ports within the group address range, which may belong to different VLANs. Profile is used to specify a group range for SVGL. Only multicast flow within this range can be forwarded across VLANs. The other multicast flow is discarded. ● In IVGL-SVGL mode, Profile is used to specify a group range for SVGL. Multicast flow within this range is in SVGL mode and the other multicast flow is in IVGL mode. ● IPv6 multicast packets cannot be forwarded through SuperVLAN.	
Configuration Examples	The following example enables MLD Snooping IVGL mode. <pre>FS(config)# ipv6 igmp snooping ivgl</pre> The following example enables MLD Snooping SVGL mode and specifies the shared VLAN and SVGL group range as VLAN1 and profile1 respectively. <pre>FS(config)# ipv6 igmp snooping svgl FS(config)# ipv6 igmp snooping svgl profile 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

9.6 ipv6 mld snooping dyn-mr-aging-time

	Use this command to set the aging time of the dynamic multicast route port. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping dyn-mr-aging-time <i>second</i>	
	no ipv6 mld snooping dyn-mr-aging-time	
	default ipv6 mld snooping dyn-mr-aging-time	
Parameter Description	Parameter	Description
	<i>second</i>	Sets the aging time of the dynamic multicast route port, in the range from 1 to 3,600 in the unit of seconds.
Defaults	The default is 300 seconds.	
Command Mode	Global configuration mode.	
Usage Guide	The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the ipv6 PIM Hello packets within the aging timeout on this interface. Use this command to change the aging time of the routing ports learned dynamically. If the aging time is too short, routing ports will be added and deleted frequently.  By default, the dynamic learning of routing ports is enabled. If learning fails, use the show run command to check whether this function is enabled.	
Configuration Examples	The following example sets the aging time of the dynamic multicast routing port to 100 seconds. <pre>FS(config)# ipv6 mld snooping dyn-mr-aging-time 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.7 ipv6 mld snooping fast-leave enable

	Use this command to enable the MLD Snooping fast-leave function. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping fast-leave enable	
	no ipv6 mld snooping fast-leave enable	
	default ipv6 mld snooping fast-leave enable	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	The interface fast leave is that when IPv6 MLD Leave packets sent from the host are received on an interface, the interface is removed from the outgoing interface list of the corresponding forwarding entry. Then, the switch will not forward the received IPv6 MLD specific group query packets to the interface.  If there is only one receiver connected with the interface, enable the interface fast leave function to save the bandwidth and resources.	
Configuration Examples	The following example enables mld snooping fast-leave. <pre>FS(config)# ipv6 mld snooping fast-leave</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.8 ipv6 mld snooping filter

	Use this command to filter the specific multicast flows. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping filter <i>profile-number</i>	
	no ipv6 mld snooping filter	
	default ipv6 mld snooping filter	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Sets the profile number in the range from 1 to 1024.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	

Usage Guide	You can configure an MLD Profile on an interface. If the MLD Report packets are received on the interface, the layer-2 device will determine whether the multicast address to be joined the interface is within the allowed range of the MLD Profile. The specified profile must be created before using this command.	
Configuration Examples	The following example associates profile1 with the interface GigabitEthernet 0/1. FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ipv6 mld snooping filter 1	
Related Commands	Command	Description
	ipv6 mld profile	Creates a profile.
Platform Description	N/A	

9.9 ipv6 mld snooping host-aging-time

	Use this command to set the aging time of the dynamic member port. Use the no form of this command to cancel this configuration. Use the default form of this command to restore the default setting.	
	ipv6 mld snooping host-aging-time <i>seconds</i>	
	no ipv6 mld snooping host-aging-time	
	default ipv6 mld snooping host-aging-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the aging time of the dynamic member port, in seconds, ranging from 1-65,536 in the unit of seconds.
Defaults	The default aging time of the dynamic member port is 260 seconds.	
Command Mode	Global configuration mode	
Usage Guide	The switch will remove the dynamic multicast router interface from the router interface list if it fails to receive the MLD general group query packets or the IPv6 PIM Hello packets within the aging timeout on this interface. When the MLD Snooping is enabled, the port that receives the MLD Report packet will learn to be a dynamic member port. The default aging time of such dynamic member port is 260 seconds. You can use this command to adjust the aging time. This configuration takes effect after the port receives the the next Report packet. The aging time of the dynamic member port should be longer than the query interval.	
Configuration Examples	The following example sets the aging time of the dynamic member port to 30 seconds:	
	FS(config)# ipv6 mld snooping host-aging-time 30	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.10 ipv6 mld snooping max-groups

	Use this command to set the maximum group allowed to join the interface dynamically. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping max-groups <i>number</i>	
	no ipv6 mld snooping max-groups	
	default ipv6 mld snooping max-groups	
Parameter Description	Parameter	Description
	<i>number</i>	The number of groups, in the range from 0 to 65,536
Defaults	The default is 65,536.	
Command Mode	Interface configuration mode	
Usage Guide	With this command configured, when the group number exceeds the specified range on the interface, the switch will not receive and deal with the MLD Report packets. The multicast groups are counted based on VLANs of an interface. If the interface has 3 VLANs, the counting result is 3 instead of 1 when an FF15::100 multicast request is received by all the VLAN.	
Configuration Examples	The following example sets the maximum 100 multicast group on the interface GigabitEthernet 0/1. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ipv6 mld snooping max-groups 100</pre>	
Related Commands	Command	Description
	ipv6 mld snooping filter	Filters the multicast group on the interface.
Platform Description	N/A	

9.11 Ipv6 mld snooping mrouter learn

	Use this command to enable the switch to dynamically learn MLD query or PIM packets to identify the mrouter interface automatically. Use the no form of this command to disable this function.

	Use the default form of this command to restore the default setting.	
	ipv6 mld snooping [vlan vid] mrouter learn	
	no ipv6 mld snooping [vlan vid] mrouter learn	
	default ipv6 mld snooping [vlan vid] mrouter learn	
Parameter Description	Parameter	Description
	vlan vid	VLAN ID, in the range from 1 to 4094
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The routing interface is the interface of the multicast device connected with the peer device. By default, the dynamically learned routing interface is enabled on the layer-2 multicast device. Use the no option to disable this function and clear all dynamically-learned routing interfaces.  With the source port check enabled, only the multicast flow through the mroute interface are valid and forwarded to the registered interface on the layer-2 multicast device. Those multicast flow through the non-mroute interface are invalid and will be discarded.	
Configuration Examples	The following example enables the dynamic multicast routing port learning function for VLAN1. <pre>FS(config)# no ipv6 mld snooping mrouter learn FS(config)# ipv6 mld snooping vlan 1 mrouter learn</pre>	
Related Commands	N/A	

9.12 ipv6 mld snooping query-max-response-time

	Use this command to set the maximum response time of the MLD general query packet.	
	Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping query-max-response-time seconds	
	no ipv6 mld snooping query-max-response-time	
	default ipv6 mld snooping query-max-response-time	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the maximum response time of the MLD general query packet in the range from 1 to 65,535 in the unit of seconds.
Defaults	The default is 10 seconds.	

Command Mode	Global configuration mode	
Usage Guide	Upon receiving the MLD general query packets, the Layer-2 multicast device updates the aging timer of all member ports. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list. Upon receiving the MLD specific group query packets, the Layer-2 multicast device enables the aging timer of all member ports in this specific group. The time of the timer is the longest response value. When the timer value decreases to 0, it indicates that there is no member receiving the multicast flow on the interface, and the Layer-2 device removes this interface from the MLD Snooping forwarding list. For the source query packets of the MLD specific group, the timer is not updated. The configured maximum response time is effective after another query packet is received.	
Configuration Examples	The following example sets the maximum response time of the MLD general query packet to 100 seconds. <pre>FS(config)# ipv6 mld snooping query-max-response-time 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.13 ipv6 mld snooping source-check port

	Use this command to enable the MLD source-check port. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping source-check port	
	no ipv6 mld snooping source-check port	
	default ipv6 mld snooping source-check port	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The source-check port is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The MLD Snooping source port check function is to limit the MLD multicast flow through the interace strictly. With the source port check disabled, all video flow are illegal and forwarded to the registered member port according to the MLD Snooping forwarding list. With the MLD Snooping source port check enabled, only the	

	multicast flow through the mroute interface is legal and forwarded to the registered interface by the layer-2 multicast device; and the multicast flow through the non-mroute interface are illegal and discarded. This command is used to enabled the source port check globally. Once this function is enable, all multicast flow must come from the mroute interface, or they'll be discarded.	
Configuration Examples	The following example enables MLD Snooping source-check port. <pre>FS(config)# ipv6 mld snooping source-check port</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.14 ipv6 mld snooping suppression enable

	Use this command to enable the MLD Snooping suppression. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping suppression enable	
	no ipv6 mld snooping suppression enable	
	default ipv6 mld snooping suppression enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The MLD Snooping suppression function is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	With the IPv6 MLD Snooping suppression function enabled, within the query interval, the layer-2 device will only forward the first received MLD Report packet in an IPv6 multicast group to the layer-3 device, but not the other MLD Report packets in the same IPv6 multicast group, reducing the packet number in the network. This command is used to enable the IPv6 MLD Snooping suppression, and only the MLDv1 Report packets are suppressed rather than the MLDv2 Report packets.	
Configuration Examples	The following example enables MLD Snooping suppression. <pre>FS(config)# ipv6 mld snooping suppression enable</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

9.15 ipv6 mld snooping svgl profile

	Use this command to specify the group address range to be in the SVGL mode. Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping svgl profile <i>profile-number</i>	
	no ipv6 mld snooping svgl profile	
	default ipv6 mld snooping svgl profile	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Sets the profile number, in the range from 1 to 1024.
Defaults	No profiles are associated with SVGL by default.	
Command Mode	Global configuration mode	
Usage Guide	With the SVGL mode or IVGL-SVGL mode configured for the MLD Snooping working mode, a profile shall be associated with the IVGL for the purpose of specifying the group address range in the SVGL mode. That is to say, the member port of the multicast forwarding entry can be forwarded across the VLANs, while the member ports of the corresponding multicast forwarding entries within other multicast address range must belong to the same VLAN. By default, no profile is associated, which means that apply no multicast group in the SVGL mode.	
Configuration Examples	The following example specifies the SVGL mode application range as the profile 2 group address range. <pre>FS(config)# ipv6 mld snooping svgl profile 2</pre>	
Related Commands	Command	Description
	ipv6 mld snooping ivgl	Enables the MLD Snooping and set the ivgl mode.
	ipv6 mld snooping ivgl-svgl	Enables the MLD Snooping and set the ivgl-svgl mode.
Platform	N/A	
Description		

9.16 ipv6 mld snooping svgl vlan

	Use this command to specify the shared VLAN in MLD Snooping SVGL mode. Use the no or default form of this command to restore the default setting.
	ipv6 mld snooping svgl vlan <i>vid</i>
	no ipv6 mld snooping svgl vlan

	default ipv6 mld snooping svgl vlan	
Parameter Description	Parameter	Description
	<i>vid</i>	The VLAN ID, in the range from 1 to 4094.
Defaults	The default is 1.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to specify the SVGL shared VLAN if MLD Snooping is running in SVGL or IVGL-SVGL mode.	
Configuration Examples	The following example sets the shared VLAN in MLD Snooping SVGL mode to 5.	
	FS(config)# ipv6 mld snooping svgl vlan 5	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.17 ipv6 mld snooping vlan

	Use this command to enable the MLD Snooping function for the specified VLAN. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	ipv6 mld snooping vlan <i>vid</i>	
	no ipv6 mld snooping vlan <i>vid</i>	
	default ipv6 mld snooping vlan <i>vid</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094.
Defaults	The MLD Snooping function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	By default, the MLD Snooping is enabled in all VLANs. You can disable the MLD Snooping for the specified VLAN.	
Configuration	The following example disables the MLD Snooping function in VLAN 2 in IVGL mode.	

Examples	FS(config)# ipv6 mld snooping ivgl	
	FS(config)# no ipv6 mld snooping vlan 2	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.18 ipv6 mld snooping vlan mrouter interface

	Use this command to set the static mrouter interface.	
	Use the no or default form of this command to restore the default setting.	
	ipv6 mld snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>	
	no ipv6 mld snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>	
	default ipv6 mld snooping vlan <i>vid</i> mrouter interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094.
	<i>interface-type</i> <i>interface-number</i>	The interface number
Defaults	No static mrouter interface is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the static mrouter interface for the purpose that all IPv6 multicast data received on the switch can be forwarded. With the source port check function enabled, only the multicast flow through the mroute interface can be forwarded.	
Configuration Examples	The following example sets a multicast routing port. FS(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet 0/1	
Related Commands	Command	Description
	ipv6 mld snooping source-check port	Sets the multicast source port check.
Platform Description	N/A	

9.19 ipv6 mld snooping vlan static interface

	Use this command to set a static member port to receive the multicast flow for the purpose of preventing the port from being influenced by the MLD Report packets with the MLD Snooping enabled. Uses the no form of this command to restore the default setting.	
	ipv6 mld snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i>	
	no ipv6 mld snooping vlan <i>vid</i> static <i>group-address</i> interface <i>interface-type interface-number</i>	
Parameter Description	Parameter	Description
	<i>vid</i>	VLAN ID, in the range from 1 to 4094. The default is 1.
	<i>group-address</i>	The multicast address
	<i>interface-type interface-number</i>	The interface number
Defaults	No static member port is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to set the interface as the member port of multiple static multicast addresses.	
Configuration Examples	The following example sets the interface gigabitEthernet 0/1 as the static member port of the FF88::1 group. FS(config)# ipv6 mld snooping vlan 1 static FF88::1 interface gigabitEthernet 0/1	
Related Commands	Command	Description
	ipv6 mld snooping vlan mrouter interface	Sets the mrouter interface.
Platform Description	N/A	

9.20 permit

	Use this command to allow the multicast flow profile within the specified range in the profile configuration mode.	
	permit	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default profile action is deny .	
Command Mode	Profile configuration mode	

Usage Guide	Before configuring this command, use the range command to set the multicast range first.	
Configuration Examples	The following example allows the multicast flow profile within the range from FF15::1 to FF15::100 to be forwarded only. <pre>FS(config)# ipv6 mld snooping profile 1 FS(config-profile)# range FF15::1 FF15::100 FS(config-profile)# permit</pre>	
Related Commands	Command	Description
	ipv6 mld profile	Creates one profile.
	range	Sets the multicast address range.
	deny	Sets the profile action deny.
Platform Description	N/A	

9.21 range

	Use this command to specify the profile multicast flow range, which can be one single multicast address, or can be the multicast address within the specified range when configuring a profile in the profile configuration mode.	
	range <i>low-ipv6-address</i> [<i>high-ip-address</i>]	
Parameter Description	Parameter	Description
	<i>low-ip-address</i>	The low address within the specified range
	<i>high-ip-address</i>	The high address within the specified range
Defaults	No range is defined by default.	
Command Mode	Profile configuration mode	
Usage Guide	The value of low-ipv6-address shall be smaller than the one of high-ipv6-address. With the address range configured, an action shall be specified, and the default profile action is deny.	
Configuration Examples	The following example creates the multicast flow profile within the range from FF15::1 to FF15::100. <pre>FS(config)# ipv6 mld snooping profile 1 FS(config-profile)# range FF15::1 FF15::100 FS(config-profile)# permit</pre>	

Related Commands	Command	Description
	ipv6 mld profile	Creates one profile.
	deny	Sets the profile action deny.
	permit	Sets the profile action permit.
Platform Description	N/A	

9.22 show ipv6 mld profile

	Use this command to display the related MLD profile configuration.	
	show ipv6 mld profile <i>profile-number</i>	
Parameter Description	Parameter	Description
	<i>profile-number</i>	Profile number in the range from 1 to 1024
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the related MLD profile configuration.	
Configuration Examples	The following example displays the MLD profile configuration. <pre> FS# show ipv6 mld profile ipv6 mld profile 1 permit range FF15::1 FF15::100 ipv6 mld profile 2 deny range FF88::1 FF88::100 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.23 show ipv6 mld snooping

	Use this command to display the related MLD Snooping information.	
	show ipv6 mld snooping [gda-table interfaces <i>interface-type interface-number</i> mrouter statistics [vlan <i>vid</i>] vlan <i>vid</i>]	
Parameter Description	Parameter	Description
	gda-table	Displays the multicast forwarding rule table.
	Interfaces <i>interface-type interface-number</i>	Displays the MLD Snooping filtering configuration.
	mrouter	Displays the information about mrouter interface.
	statistics	Displays the MLD Snooping statistics.
	vlan <i>vlan-id</i>	Displays the MLD Snooping information of the specified vlan.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the related MLD Snooping information.	
Configuration Examples	The following example displays the MLD Snooping configurations. <pre> In IVGL mode: FS#show ipv6 mld snooping MLD-snooping mode: IVGL Source port check: Disable MLD Fast-Leave: Disable MLD Report suppress: Disable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds) vlan 1 ----- MLD Snooping state: Enabled Multicast router learning mode: Enable MLD Fast-Leave: Enabled MLD VLAN Mode: STATIC In SVGL mode: FS#show ipv6 mld snooping MLD-snooping mode: SVGL SVGL vlan: 1 </pre>	

	SVGL profile number: 1 Source port check: Disable MLD Fast-Leave: Disable MLD Report suppress: Disable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds) In IVGL-SVGL mode: FS#show ipv6 mld snooping MLD-snooping mode: IVGL-SVGL SVGL vlan: 1 SVGL profile number: 1 Source port check: Disable MLD Fast-Leave: Disable MLD Report suppress: Disable Query Max Response Time: 10 (Seconds) Dynamic Mroute Aging Time: 300(Seconds) Dynamic Host Aging Time: 260(Seconds) vlan 1 ----- MLD Snooping state: Enabled Multicast router learning mode: Enable MLD Fast-Leave: Enabled MLD VLAN Mode: STATIC	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10 MSDP Commands

10.1 clear ip msdp peer

	Use this command to clear specific MSDP peer. This will clear the connection to the MSDP peer and then reestablish the connection to MSDP peer. The statistics of MSDP peer will be cleared at the same time.	
	clear ip msdp peer <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the TCP connection to the specified MSDP peer and clear all the MSDP peer statistics.	
Configuration Examples	The following example clears MDSP peer of 218.14.5.23. <pre>FS# clear ip msdp peer 218.14.5.23</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.2 clear ip msdp sa-cache

	Use this command to clear SA cache entries.	
	clear ip msdp sa-cache [<i>group-address</i>]	
Parameter Description	Parameter	Description
	<i>group-address</i>	Group address
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	Use this command to clear the SA cache entries learned from MSDP peer. If no multicast group address is specified, all SA cache entries will be cleared. After SA cache entries are cleared, the MSDP device will need to relearn SA messages.	
Configuration Examples	The following example clears the SA cache entries with the multicast group 224.1.1.1. <pre>FS# clear ip msdp sa-cache 224.1.1.1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.3 clear ip msdp statistics

	Use this command to clear the statistics of MSDP peers without resetting the TCP sessions.	
	clear ip msdp statistics [<i>peer-address</i>]	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer whose statistics counters, reset count, and input/output count will be cleared.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the statistics of MSDP peers and view the new statistics of MSDP peers. This command can clear the statistics of one or more MDSP peers without resetting the MSDP peer.	
Configuration Examples	The following example clears the statistics of the MSDP peer with IP address being 61.83.1.52. <pre>FS# clear ip msdp statistics 61.83.1.52</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.4 ip msdp default-peer

	Use this command to define a default MSDP peer. Use no or default form of this command to restore the default setting.	
	ip msdp default-peer <i>peer-address</i> [prefix-list <i>prefix-list-name</i>] no ip msdp default-peer <i>peer-address</i> default ip msdp default-peer <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
	prefix-list <i>prefix-list-name</i>	Specifies the BGP prefix list.
Defaults	By default, no default MSDP peer is configured.	
Command Mode	Global configuration mode	
Usage Guide	The RPF-Peer calculation rule for the specified RP address may leads the loss of RPF-Peer information, which causes that the SA messages are dropped directly without the Peer-RPF check. With a default peer configured, the SA messages are ensured to pass the Peer-RPF check, so that the local host could accept the SA messages to learn the multicast source information carried by the SA messages. If "prefix-list prefix-list-name" is not specified, all SA messages from the default MSDP peer will be accepted. If "prefix-list prefix-list-name" is specified, only the SA messages from the RP specified by prefix-list prefix-list-name will be accepted. If "prefix-list prefix-list-name" is specified but the prefix list is not configured, all SA messages from this default MSDP peer will be accepted.	
Configuration Examples	The following example configures 172.16.33.1 as the default peer. <pre>FS(config)# ip msdp peer 172.16.33.1 FS(config)# ip msdp peer 172.16.34.2 FS(config)# ip msdp default-peer 172.16.33.1</pre>	
Related Commands	Command	Description
	ip msdp peer	Creates MSDP peer.
Platform Description	This command is supported only on layer-3 device.	

10.5 ip msdp description

	Use this command to add descriptive information for MSDP peer. Use no or default form of this command to restore the default setting.

	ip msdp description <i>peer-address text</i>	
	no ip msdp description <i>peer-address</i>	
	default ip msdp description <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
	<i>text</i>	Descriptive information for MSDP peer
Defaults	No descriptive information is configured for MSDP peer.	
Command Mode	Global configuration mode	
Usage Guide	The administrator can configure descriptive information for MSDP peers in order to identify them conveniently. If the descriptive information A is specified for an MSDP peer, A is displayed. If no descriptive information is specified, "No description" is displayed.	
Configuration Examples	The following example configures the descriptive information for peer 172.17.1.2 as "customer-a". FS(config)# ip msdp description 172.17.1.2 customer-a	
Related Commands	Command	Description
	show ip msdp peer	Displays the descriptive information for MSDP peer.
Platform Description	This command is supported only on L3 devices.	

10.6 ip msdp filter-sa-request

	Use this command to filter the SA request messages sent from MSDP peer. Use the no or default form of this command to restore the default setting.	
	ip msdp filter-sa-request <i>peer-address [list access-list]</i>	
	no ip msdp filter-sa-request <i>peer-address</i>	
	default ip msdp filter-sa-request <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
	list <i>access-list</i>	The standard IP access list number or name for limiting multicast group addresses
Defaults	All SA request messages from MSDP peer will be accepted and replied.	

Command Mode	Global configuration mode	
Usage Guide	Use this command to control which SA request messages will be accepted and replied. If no access list is specified, all SA request messages will be ignored. If a null access list is specified, all SA request messages will be ignored. If an access list is specified, only the SA request messages from the multicast group permitted by the access list will be accepted, and other messages will be ignored.	
Configuration Examples	The following example configures to filter SA request messages from peer 172.16.223.1 and only accept SA request messages with group address falling within 224.0.1.0-224.0.1.255. FS(config)# ip msdp filter-sa-request 172.16.223.1 list 1 FS(config)# access-list 1 permit 224.0.1.1 0.0.0.255	
Related Commands	Command	Description
	ip msdp peer	Creates MSDP peer.
Platform Description	This command is supported only on L3 devices.	

10.7 ip msdp mesh-group

	Use this command to configure a MSDP peer to be a member of a mesh group. Use the no form of this command to remove the configuration. Use the default form of this command to restore the default settings.	
	ip msdp mesh-group <i>mesh-name peer-address</i>	
	no ip msdp mesh-group <i>mesh-name peer-address</i>	
	default ip msdp mesh-group <i>mesh-name peer-address</i>	
Parameter Description	Parameter	Description
	<i>mesh-name</i>	Name of mesh group, case sensitive
	<i>peer-address</i>	IP address of the MSDP peer to be a member of mesh group.
Defaults	No mesh group will be created, and MSDP peers do not belong to any mesh group.	
Command Mode	Global configuration mode	
Usage Guide	All MSDP peers in the mesh group shall be fully meshed, namely MSDP peer relationship has been established between every two members in the mesh group. The SA received by one member of the mesh group won't be forwarded to other members in the same mesh group, thus reducing SA flooding and simplify Peer-RPF forwarding.	

Configuration Examples	The following example configures MSDP peer at address 192.168.1.3 to be a member of the mesh group named "msdp-mesh". FS(config)# ip msdp mesh-group <i>msdp-mesh 192.168.1.3</i>	
Related Commands	Command	Description
	show ip msdp mesh-group	Displays the information of mesh group.
Platform Description	This command is supported only on L3 devices.	

10.8 ip msdp originator-id

	Use this command to allow a speaker that originates a SA message to use the IP address of the interface as the originator address in the SA message. Use the no form of this command to remove this configuration. Use the default form of this command to restore the default setting.	
	ip msdp originator-id <i>interface-type interface-number</i>	
	no ip msdp originator-id	
	default ip msdp originator-id	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number
Defaults	By default, the originator address in SA messages will be the RP address configured by PIM.	
Command Mode	Global configuration mode	
Usage Guide	The master IP address of this interface will be used as the originator address in the SA messages. If no IP address is configured for this interface, or the interface is shut down, then the originator address in the SA messages won't use the master IP address of this interface, but use the RP address configured by PIM. Under certain circumstances, you may expect to change the originator address in SA messages, such as during Anycast-RP deployment. By this time, you can use this command to modify the originator address in SA messages.	
Configuration Examples	The following example uses the IP address of Loopback0 as the RP address in SA messages. <pre>FS(config)# ip msdp originator-id loopback0</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.9 ip msdp password

	Use this command to enable MD5 encryption of the TCP connection between MSDP peers. Use the no or default form of this command to restore the default setting.	
	ip msdp password peer <i>peer-address</i> [<i>encryption-type</i>] <i>string</i>	
	no ip msdp password peer <i>peer-address</i>	
	default ip msdp password peer <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer
	<i>encryption-type</i>	Grade of password: 0 (lowest level)-7 (highest level). Currently, only 0 and 7 are supported. The default encryption type is 0.
	<i>string</i>	The password used for TCP MD5 authentication. Range: up to 80 characters when the encryption type is 0; up to 160 characters when the encryption type is 7.
Defaults	MD5 encryption of the TCP connection between MSDP peers is disabled.	
Command Mode	Global configuration mode	
Usage Guide	When it is needed to authenticate the MSDP peers, you can enable MD5 encryption of TCP connection between MSDP peers. In such a case, two interconnected MSDP peers must be configured with MD5 authentication with same password, or else the connection will fail. If the password is configured or changed, the local MSDP device won't terminate the current session, but will try to use the new password to maintain the current session until timeout. If you have configure the password locally for the MSDP peer but no password is configured on MSDP, the following warning message will be displayed on the console: <pre>%TCP-6-BADAUTH: MD5 digest NOT expected but found (200.200.200.6, 39996)->(200.200.200.16, 639)</pre> If different MD5 passwords are configured between MSDP peers, the following warning message will be displayed on the console: <pre>%TCP-6-BADAUTH: MD5 digest failed for (200.200.200.6, 12302)->(200.200.200.16, 639)</pre>  If the encryption type is 0, the encryption key for TCP is the string entered in the console. That is, this type of encryption is supported when FS Networks MSDP devices communicates with those from other vendors. Thus, this encryption type is recommended for mutual communication between devices from different	

	vendors.  If the encryption type is 7, the entered encryption key must be even and not less than 4. Different from type 0, the encryption key is not the string entered in the console. Instead, it is a new string computed by FS-defined algorithm. In addition, our algorithm is different from other private vendor-specific algorithms. Therefore, this encryption type is supported only when FS Networks devices are mutually connected.	
Configuration Examples	The following example configures the MD5 password of "test" for the MSDP peer of 10.32.43.144. <pre>FS(config)# ip msdp password peer 10.32.43.144 0 test</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.10 ip msdp peer connect-source

	Use this command to create MSDP peer. Use no or default form of this command to remove MSDP peer.	
	ip msdp peer <i>peer-address</i> connect-source <i>interface-type interface-number</i>	
	no ip msdp peer <i>peer-address</i>	
	default ip msdp peer <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer The peer MSDP device uses this address to communicate with the local MSDP device for TCP connection.
	<i>interface-type</i> <i>interface-number</i>	Interface type and interface number. The local MSDP device uses the main address of this interface as the source IP for the TCP connection to the remote MSDP peer. Loopback interface is recommended. If no IP address is configured for this interface, or the interface is shut down, then MSDP peer relation cannot be established.
Defaults	No MSDP peer is created.	
Command Mode	Global configuration mode	
Usage Guide	To enable MSDP, MSDP peer must be created.	

Configuration Examples	The following example configures the main address of interface loopback 0 as the source address for establishing MSDP peer relation with 192.168.5.1. FS(config)# ip msdp peer 192.168.5.1 connect-source loopback 0	
Related Commands	Command	Description
	show ip msdp peer	Displays the information about MSDP peer.
Platform Description	This command is supported only on L3 devices.	

10.11 ip msdp redistribute

	Use this command to configure which (S, G) entries from the multicast routing table can be advertised to MSDP peers. Use the no form of this command to remove this configuration. Use the default form of this command to restore the default settings.	
	ip msdp redistribute [list <i>access-list-name</i>] [route-map <i>route-map</i>]	
	no ip msdp redistribute	
	default ip msdp redistribute	
Parameter Description	Parameter	Description
	list <i>access-list-name</i>	Number or name of an extended IP access list that controls which multicast routes (S, G) can be advertised.
	route-map <i>route-map</i>	Defines route-map.
Defaults	All multicast sources (S, G) registered on the local RP will be advertised.	
Command Mode	Global configuration mode	
Usage Guide	After redistribution filtering is configured, the (S, G) information from the local AS or the other AS can be added to the MSDP only through redistribution filtering. If " list <i>access-list-name</i> " is specified, only those matched multicast routes (S, G) will be advertised. If " route-map <i>map-name</i> " is specified, only multicast routes (S, G) matching the criteria given in " <i>map-name</i> " will be advertised. If two keywords are specified, then multicast routes (S, G) matching all conditions will be advertised. If the " ip msdp redistribute " command is configured with no keywords, no multicast sources will be advertised.	
Configuration Examples	The following example configures to only advertise multicast routes with multicast source being 200.200.200.0/24 and group address being 225.1.1.0/24. Router(config)# ip msdp redistribute list 100	

	Router(config)# ip access-list extended 100 Router(config-ext-nacl)# permit ip 200.200.200.0 0.0.0.255 225.1.1.0 0.0.0.255	
Related Commands	Command	Description
	ip msdp sa-filter in	Configures the incoming filter for SA messages.
	ip msdp sa-filter out	Configures the outgoing filter for SA messages.
Platform Description	This command is supported only on L3 devices.	

10.12 ip msdp sa-filter in

	Use this command to configure an incoming filter for SA messages. Use the no or default form of this command to remove the incoming filter.	
	ip msdp sa-filter in <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	
	no ip msdp sa-filter in <i>peer-address</i>	
	default ip msdp sa-filter in <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer
	list <i>access-list</i>	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.
	route-map <i>route-map</i>	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
	rp-list <i>rp-access-list</i>	Number or name of standard access list that controls RPs.
	rp-route-map <i>rp-route-map</i>	Specify the name of route map for RP; only the SA messages matching rp-map-name can be accepted.
Defaults	All incoming SA messages will be accepted without filtering.	
Command Mode	Global configuration mode	
Usage Guide	If the command is configured, but no access list or route map is specified, all incoming SA messages will be filtered. If only the list keyword or the route-map keyword is used, the multicast source (S, G) in SA messages matching the criteria corresponding to this keyword will be accepted. If only the rp-list keyword or the rp-route-map keyword is used, the SA message will be accepted if the RP address carried in SA message matches the criteria corresponding to this keyword. If two or more keywords of list, route-map, rp-list and rp-route-map are used, the SA message will be accepted if any multicast source (S, G) in SA message meet the criteria corresponding to all keywords.	

Configuration	The following example configures that all SA messages from the peer of 10.234.1.43 will be filtered.	
Examples	<pre>FS(config)# ip msdp peer 10.234.1.43 FS(config)# ip msdp sa-filter in 10.234.1.43</pre>	
Related Commands	Command	Description
	ip msdp peer	Configures MSDP peer.
	ip msdp sa-filter-out	Configures the outgoing filter for SA messages received from MSDP peers.
Platform Description	This command is supported only on L3 devices.	

10.13 ip msdp sa-filter out

	Use this command to configure an outgoing filter for SA messages. Use the no or default form of this command to remove the outgoing filter.	
	ip msdp sa-filter out <i>peer-address</i> [list <i>access-list</i>] [route-map <i>route-map</i>] [rp-list <i>rp-access-list</i>] [rp-route-map <i>rp-route-map</i>]	
	no ip msdp sa-filter out <i>peer-address</i>	
	default ip msdp sa-filter out <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer
	list <i>access-list</i>	Number or name of an extended IP access list that controls which multicast routes (S, G) can be received.
	route-map <i>route-map</i>	Specify the name of route-map; only SA messages matching the criteria given in "map-name" can pass through.
	rp-list <i>rp-access-list</i>	Number or name of standard access list that controls RPs.
	rp-route-map <i>rp-route-map</i>	Specify the name of route map for RP; only the SA messages matching rp-map-name can be accepted.
Defaults	All SA messages received will be forwarded to the MSDP peer.	
Command Mode	Global configuration mode	
Usage Guide	If the command is configured, but no access list or route map is specified, all SA messages won't be forwarded to this MSDP peer. If only one keyword of list , route-map , rp-list and rp-route-map is used, the multicast source pair (S, G) will be forwarded to this MSDP peer if the criteria corresponding to this keyword are met. If two or more keywords of list , route-map , rp-list and rp-route-map are used, the (S, G) pair will only be	

	forwarded to this MSDP peer if criteria corresponding to all keywords are met.	
Configuration Examples	The following example allows only multicast sources that pass access list 100 to be forwarded to the peer of 10.234.1.43. <pre>FS(config)# ip msdp peer 10.234.1.43 FS(config)# ip msdp sa-filter out 10.234.1.43 list 100 FS(config)# access-list 100 permit ip 10.211.0.0 0.0.255.255 224.12.0.0 0.0.255.255</pre>	
Related Commands	Command	Description
	ip msdp peer	Configures MSDP peer.
	ip msdp sa-filter-in	Configures the incoming filter for SA messages received from MSDP peers.
Platform Description	This command is supported only on L3 devices.	

10.14 ip msdp sa-limit

	Use this command to configure the allowable maximum number of Source-Active (SA) cache entries from a MSDP peer. Use the no or default form of this command to restore the default settings.	
	ip msdp sa-limit <i>peer-address sa-limit</i>	
	no ip msdp sa-limit <i>peer-address</i>	
	default ip msdp sa-limit <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of MSDP peer
	<i>sa-limit</i>	Maximum number of SA messages from an MSDP peer allowed in the SA cache
Defaults	The maximum number of SA messages from an MSDP peer allowed in the SA cache is not limited.	
Command Mode	Global configuration mode	
Usage Guide	It is suggested to configure this command on all MSDP peers to prevent SA flooding attacks from MSDP peers. When the local device has learned A (quantity) SA entries from an MSDP peer, and A is greater than B (the SA limit), the SA entries from this peer will not be cleared at once. Instead, the aging mechanism (no more than 135 seconds) will lower A to B. That is, this command is not effective immediately. It aims to saving effective multicast information best to raise networking productivity. If you want to clear the SA entries in such case, use the clear ip msdp sa-cache command.	

Configuration Examples	The following example configures the SA message limit to 100 for the MSDP peer with IP address being 172.16.3.1. FS(config)# ip msdp sa-limit 172.16.3.1 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.15 ip msdp shutdown

	Use this command to shut down the connection to MSDP peer. Use the no or default form of this command to restore the default settings.	
	ip msdp shutdown <i>peer-address</i>	
	no ip msdp shutdown <i>peer-address</i>	
	default ip msdp shutdown <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
Defaults	The connection to peer is not shut down.	
Command Mode	Global configuration mode	
Usage Guide	Only the TCP connection to the specified MSDP peer will be shut down. Neither the MSDP peer nor its configurations will be cleared.	
Configuration Examples	The following example shuts down the MSDP peer at IP address 192.168.7.20. FS(config)# ip msdp shutdown 192.168.7.20	
Related Commands	Command	Description
	ip msdp peer	Creates MSDP peer.
Platform Description	This command is supported only on L3 devices.	

10.16 ip msdp timer

	Use this command to configure the interval for timer re-connection. Use the no or default form of this command to restore the default settings.	
	ip msdp timer <i>interval</i>	
	no ip msdp timer	
	default ip msdp timer	
Parameter Description	Parameter	Description
	<i>interval</i>	Interval for timer re-connection, within the range from 1 to 60 in the unit of seconds
Defaults	The default interval is 30 seconds.	
Command Mode	Global configuration mode	
Usage Guide	By default, the interval for timer re-connection is 30 seconds, that is, the peer in active end can initiate only one TCP connection within 30 seconds. In certain applications, the interval is expected to be decreased in order to accelerate convergence of MSDP peering relation.	
Configuration Examples	The following example sets the interval for timer re-connection to 20 seconds. <pre>FS(config)# ip msdp timer 20</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.17 ip msdp ttl-threshold

	Use this command to limit the TTL value of multicast data packets carried in SA messages in order to limit the transmission of multicast packets. Use the no or default form of this command to restore to the default settings.	
	ip msdp ttl-threshold <i>peer-address ttl-value</i>	
	no ip msdp ttl-threshold <i>peer-address</i>	
	default ip msdp ttl-threshold <i>peer-address</i>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer

	<i>ttl-value</i>	TTL value in the range from 0 to 255
Defaults	TTL threshold is 0 by default.	
Command Mode	Global configuration mode	
Usage Guide	This command limits multicast data packets which are sent in data-encapsulated SA messages. Only multicast packets with an IP-header TTL greater than or equal to the <i>ttl-value</i> will be sent to the MSDP peer. If the TTL value of multicast data is less than the threshold configured, then the multicast data will be separated from SA messages and discarded, and the SA messages without multicast data will be sent to the MSDP peer. This command only limits the transmission of multicast data in SA messages without compromising the transmission of multicast sources in SA messages	
Configuration Examples	The following example configures the TTL threshold for peer at IP address 192.168.10.1 to 8 hops: <pre>FS(config)# ip msdp ttl-threshold 192.168.10.1 8</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.18 ip msdp peer-limit

	Use this command to set the upper limit of MSDP peers. Use the no form of this command to remove the configuration. Use the default form of this command to restore the default settings.	
	ip msdp peer-limit <i>peer-limit</i>	
	no ip msdp peer-limit	
	default ip msdp peer-limit	
Parameter Description	Parameter	Description
	<i>peer-limit</i>	The upper limit of MSDP peers, in the range from 1 to 128.
Defaults	The default is 64.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to set the upper limit of MSDP peers. If the number of existing MSDP peers exceeds the upper limit to be configured, you should delete some peers, or the configuration will fail.	

Configuration	The following example sets the upper limit of MSDP peers to 128.
Examples	FS(config)# ip msdp peer-limit 128
Platform	
Description	This command is supported only on L3 devices.

10.19 ip msdp global-sa-limit

	Use this command to configure the maximum SA cache. Use the no form of this command to remove the configuration. Use the default form of this command to restore the default settings.	
	ip msdp global-sa-limit <i>sa-limit</i>	
	no ip msdp global-sa-limit <i>sa-limit</i>	
	default ip msdp global-sa-limit <i>sa-limit</i>	
Parameter		
Description	Parameter	Description
	<i>sa-limit</i>	The maximum SA cache, in the range from 1 to 4,096
Defaults	The default SA cache is 1,024.	
Command	Global configuration mode	
Mode		
Usage Guide	This command is used to set the maximum SA cache. It's recommended to configure it at the beginning of startup. When MSDP is running, the increase in maximum SA cache has no influence upon the previously learned entries; the decrease in maximum SA cache will clear all entries learned before and start caching again.	
Configuration	The following example sets the maximum SA cache to 4,096.	
Examples	FS(config)# ip msdp global-sa-limit 4096	
Platform		
Description	This command is supported only on L3 devices.	

10.20 show ip msdp count

	Use this command to display the number of sources and groups originated in SA messages and the number of SA messages from an MSDP peer in the SA cache.	
	show ip msdp count [<i>as-number</i>]	
Parameter		
Description	Parameter	Description
	<i>as-number</i>	Displays the number of sources and groups originated in SA messages from

		the specified autonomous system number.								
Defaults	N/A									
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode									
Usage Guide	N/A									
Configuration Examples	FS# sh ip msdp count SA State per Peer Counters, <Peer>: <# SA learned> 1.1.1.2 : 0 100.100.100.14 : 0 100.100.100.15 : 0 100.100.100.200: 0 200.200.200.2 : 2 200.200.200.3 : 0 200.200.200.6 : 0 200.200.200.13 : 0 200.200.200.66 : 0 SA State per ASN Counters, <asn>: <# sources>/<# groups> Total entries: 2 100: 1/2 . <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>200.200.200.200:2</td><td>MSDP peer with IP address 200.200.200.200; 2 SA messages in the SA cache.</td></tr><tr><td>Total entries</td><td>Total number of SA entries in the SA cache.</td></tr><tr><td>?:1/2</td><td>Unknown autonomous system: 1 source address/2 multicast group addresses</td></tr></tbody></table>		Field	Description	200.200.200.200:2	MSDP peer with IP address 200.200.200.200; 2 SA messages in the SA cache.	Total entries	Total number of SA entries in the SA cache.	?:1/2	Unknown autonomous system: 1 source address/2 multicast group addresses
Field	Description									
200.200.200.200:2	MSDP peer with IP address 200.200.200.200; 2 SA messages in the SA cache.									
Total entries	Total number of SA entries in the SA cache.									
?:1/2	Unknown autonomous system: 1 source address/2 multicast group addresses									
Related Commands	Command	Description								
	N/A	N/A								
Platform Description	This command is supported only on L3 devices.									

10.21 show ip msdp mesh-group

	Use this command to display the information of mesh group.
	show ip msdp mesh-group

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	FS# sh ip msdp mesh-group MSDP peers in each Mesh-group,<Mesh-group name>:<# peers> msdp-mesh 1.1.1.2 1.1.1.3	
	Field	Description
	msdp-mesh	Name of mesh group
	1.1.1.2	One MSDP peer under this mesh group.
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.22 show ip msdp peer

	Use this command to display detailed information about the MSDP peer.	
	show ip msdp peer [<i>peer-address</i>]	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the MSDP peer
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	

Configuration	FS#show ip msdp peer 20.0.0.1																				
Examples	MSDP PEER 20.0.0.1 (No description), AS unknown Connection status: State: Listen, Resets: 1, Connection source: GigabitEthernet 0/1 (20.0.0.2) Uptime(Downtime): 00:00:25, Message sent/received: 13/19 Input messages discarded: 0 Connection and counters cleared 00:13:25 ago Local Address of connection: 20.0.0.2 MD5 signature protection on MSDP TCP connection: enabled SA Filtering: Input (S,G) Access-list filter: None Input (S,G) route-map filter: None Input RP Access-list filter: None Input RP Route-map filter: None Output (S,G) Access-list filter: None Output (S,G) Route-map filter: None Output RP Access-list filter: None Output RP Route-map filter: None SA-Requests: Input filter: None Peer ttl threshold: 0 SAs learned from this peer: 2, SAs limit: No-limit Message counters: SA messages discarded: 0 SA messages in/out: 13/0 SA Requests discarded/in: 0/0 SA Responses out: 0 Data Packets in/out: 6/0 <table border="1"> <thead> <tr> <th>Field</th><th>Description</th></tr> </thead> <tbody> <tr> <td>MSDP Peer</td><td>IP address of MSDP peer.</td></tr> <tr> <td>AS</td><td>Autonomous system to which the MSDP peer belongs. If it is an unknown AS, "unknown" will be displayed.</td></tr> <tr> <td>State:</td><td>State of the MSDP peer.</td></tr> <tr> <td>Connection source:</td><td>Interface used to obtain the source address for TCP connection.</td></tr> <tr> <td>Uptime(Downtime):</td><td>Up time/down time of MSDP peer.</td></tr> <tr> <td>Messages sent/received:</td><td>Number of SA messages received.</td></tr> <tr> <td>SA Filtering:</td><td>SA filtering information.</td></tr> <tr> <td>SAs learned from this peer:</td><td>Number of SA entries learned from MSDP peer.</td></tr> <tr> <td>SAs limit:</td><td>SA message limit for this MSDP peer.</td></tr> </tbody> </table>	Field	Description	MSDP Peer	IP address of MSDP peer.	AS	Autonomous system to which the MSDP peer belongs. If it is an unknown AS, "unknown" will be displayed.	State:	State of the MSDP peer.	Connection source:	Interface used to obtain the source address for TCP connection.	Uptime(Downtime):	Up time/down time of MSDP peer.	Messages sent/received:	Number of SA messages received.	SA Filtering:	SA filtering information.	SAs learned from this peer:	Number of SA entries learned from MSDP peer.	SAs limit:	SA message limit for this MSDP peer.
Field	Description																				
MSDP Peer	IP address of MSDP peer.																				
AS	Autonomous system to which the MSDP peer belongs. If it is an unknown AS, "unknown" will be displayed.																				
State:	State of the MSDP peer.																				
Connection source:	Interface used to obtain the source address for TCP connection.																				
Uptime(Downtime):	Up time/down time of MSDP peer.																				
Messages sent/received:	Number of SA messages received.																				
SA Filtering:	SA filtering information.																				
SAs learned from this peer:	Number of SA entries learned from MSDP peer.																				
SAs limit:	SA message limit for this MSDP peer.																				

Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is supported only on L3 devices.	

10.23 show ip msdp rpf-peer

	Use this command to display the information about MSDP RPF peer corresponding to the specified originator address.	
	show ip msdp rpf-peer <i>ip-address</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address of the originator of SA messages
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the rpf-peer information of RP at address 1.1.1.1: <pre>FS# sh ip msdp rpf-peer 1.1.1.1 RPF peer information for 1.1.1.1 RPF peer: 200.200.200.2 RPF rule: Peer is only active peer RPF route/mask: Not-used RPF type: Not-used</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is only supported on L3 devices.	

10.24 show ip msdp sa-cache

	Use this command to display (S, G) state learned.	
	show ip msdp sa-cache [<i>group-address</i> <i>source-address</i>] [<i>group-address</i> <i>source-address</i>] [<i>as-number</i>]	

Parameter Description	Parameter	Description										
	<i>group-address</i>	Group address of the group or source about which (S, G) information is displayed										
	<i>source-address</i>	Source address of the group or source about which (S, G) information is displayed.										
	<i>as-number</i>	Autonomous system number generated by SA messages.										
Defaults	N/A											
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode											
Usage Guide	N/A											
Configuration Examples	The following example displays (S, G) state learned. FS# sh ip msdp sa-cache MSDP Source-Active Cache: 2 entries MSDP Source-Active Cache: 2 entries (200.200.200.200, 227.1.2.2), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 (200.200.200.200, 227.1.2.3), RP: 20.20.20.20, (M)BGP/AS 100, 04:17:09/00:02:05, Peer 200.200.200.2 Learned from peer 200.200.200.2, RPF peer 200.200.200.2, SAs received: 277, Encapsulated data received: 0 <table><tr><th>Field</th><th>Description</th></tr><tr><td>(200.200.200.200, 227.1.2.2)</td><td>Source address and group address.</td></tr><tr><td>RP 20.20.20.20</td><td>RP address generating SA messages.</td></tr><tr><td>MBGP/AS</td><td>The autonomous system of the RP generating SA messages is unknown.</td></tr><tr><td>04:17:09/00:02:05</td><td>The route has been cached for 4 hours 17 minutes and 9 seconds. If no SA message is received in 2 minutes and 5 seconds, it will be removed from the SA cache.</td></tr></table>		Field	Description	(200.200.200.200, 227.1.2.2)	Source address and group address.	RP 20.20.20.20	RP address generating SA messages.	MBGP/AS	The autonomous system of the RP generating SA messages is unknown.	04:17:09/00:02:05	The route has been cached for 4 hours 17 minutes and 9 seconds. If no SA message is received in 2 minutes and 5 seconds, it will be removed from the SA cache.
Field	Description											
(200.200.200.200, 227.1.2.2)	Source address and group address.											
RP 20.20.20.20	RP address generating SA messages.											
MBGP/AS	The autonomous system of the RP generating SA messages is unknown.											
04:17:09/00:02:05	The route has been cached for 4 hours 17 minutes and 9 seconds. If no SA message is received in 2 minutes and 5 seconds, it will be removed from the SA cache.											
Related Commands	Command	Description										
	N/A	N/A										
Platform Description	This command is only supported on L3 devices.											

10.25 show ip msdp sa-originated

	Use this command to display the (S, G) information to be sent by the local device. The (S, G) information has passed redistribution filtering.							
	show ip msdp sa-originated							
Parameter Description	Parameter	Description						
	N/A	N/A						
Defaults	N/A							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode							
Usage Guide	This command can be used to display the (S, G) information sent by the local device that is the RP in PIM-SM with the multicast source (S, G) registered and is configured with MSDP peer. (S, G) information displayed has passed redistribution filtering, but, whether the information can be sent to the MSDP peer requires the results of egress filtering for the information.							
Configuration Examples	The following is sample output of "show ip msdp sa-originated" command. FS# sh ip msdp sa-originated MSDP Source-Active Originated: 5 entries (192.168.23.78, 225.0.0.1), RP: 192.168.23.249 (192.168.23.79, 225.0.0.2), RP: 192.168.23.249 (192.168.23.80, 225.0.0.3), RP: 192.168.23.249 (192.168.23.81, 225.0.0.4), RP: 192.168.23.249 (192.168.23.82, 225.0.0.5), RP: 192.168.23.249 <table><tr><th>Field</th><th>Description</th></tr><tr><td>(192.168.23.78, 225.0.0.1)</td><td>The source address (the first IP address) and group address (the second IP address) of SA to be sent.</td></tr><tr><td>RP 192.168.23.249</td><td>RP address of SA sent.</td></tr></table>		Field	Description	(192.168.23.78, 225.0.0.1)	The source address (the first IP address) and group address (the second IP address) of SA to be sent.	RP 192.168.23.249	RP address of SA sent.
Field	Description							
(192.168.23.78, 225.0.0.1)	The source address (the first IP address) and group address (the second IP address) of SA to be sent.							
RP 192.168.23.249	RP address of SA sent.							
Related Commands	Command	Description						
	N/A	N/A						
Platform Description	This command is only supported on L3 devices.							

10.26 show ip msdp summary

	Use this command to display the summary information about all MSDP peers.
	show ip msdp summary

Parameter Description	Parameter			Description																																				
	N/A			N/A																																				
Defaults	N/A																																							
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																																							
Usage Guide	If the local device configured with MSDP peers is the PIM-SM Rendezvous Point (RP) and multicast sources (S,G) registers in the RP, the command will display: (S,G) to Send The displayed (S,G) have gone through redistribution filtering (command: ip msdp redistribute). However, whether these (S,G) will be delivered to MSDP peers successfully relies on the outgoing filter (command: ip msdp sa-filter out).																																							
Configuration Examples	The following example displays the summary information about all MSDP peers. <pre>FS# sh ip msdp summary</pre> Msdp Peer Status Summary <table><tr><td>Peer Address</td><td>As</td><td>State</td><td>Uptime/Downtime</td><td>Reset-Count</td><td>Sa-Count</td></tr><tr><td>Peer-description</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>200.200.200.2</td><td>100</td><td>Up</td><td>04:22:11</td><td>10</td><td>6616</td></tr><tr><td>200.200.200.3</td><td>100</td><td>Down</td><td>19:17:13</td><td>4</td><td>0</td></tr></table> peer-A <table><tr><th>Field</th><th>Description</th></tr><tr><td>Peer Address</td><td>IP address of MSDP peer</td></tr><tr><td>AS</td><td>Autonomous system to which the MSDP peer belongs</td></tr><tr><td>State</td><td>State of the MSDP peer</td></tr><tr><td>Uptime/Downtime</td><td>Up time or down time of MSDP peer</td></tr></table>						Peer Address	As	State	Uptime/Downtime	Reset-Count	Sa-Count	Peer-description						200.200.200.2	100	Up	04:22:11	10	6616	200.200.200.3	100	Down	19:17:13	4	0	Field	Description	Peer Address	IP address of MSDP peer	AS	Autonomous system to which the MSDP peer belongs	State	State of the MSDP peer	Uptime/Downtime	Up time or down time of MSDP peer
Peer Address	As	State	Uptime/Downtime	Reset-Count	Sa-Count																																			
Peer-description																																								
200.200.200.2	100	Up	04:22:11	10	6616																																			
200.200.200.3	100	Down	19:17:13	4	0																																			
Field	Description																																							
Peer Address	IP address of MSDP peer																																							
AS	Autonomous system to which the MSDP peer belongs																																							
State	State of the MSDP peer																																							
Uptime/Downtime	Up time or down time of MSDP peer																																							
Related Commands	Command			Description																																				
	N/A			N/A																																				
Platform Description	This command is only supported on L3 devices.																																							

Network Management & Monitoring Commands

1 SNMP Commands

1.1 clear snmp locked-ip

	Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures.	
	clear snmp locked-ip [ipv4 <i>ipv4-address</i> ipv6 <i>ipv6-address</i>]	
Parameter Description	Parameter	Description
	ipv4 <i>ipv4-address</i>	Clears a specified IPv4 address.
	ipv6 <i>ipv6-address</i>	Clears a specified IPv6 address.
Defaults	N/A	
Command mode	Privileged EXEC mode.	
Usage Guide	Use this command to clear the source IP addresses which are locked after continuous SNMP authentication failures. You can clear the whole source IP address table or a specific source IP address. After the source IP addresses locked are cleared, the SNMP packets with these source IP addresses could be authenticated again.	
Configuration Examples	The following example clears the whole source IP address table locked after continuous SNMP authentication failures. <pre>FS#clear snmp locked-ip</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.2 no snmp-server

	Use this command to disable the SNMP agent function.	
	no snmp-server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	SNMP agent is enabled by default.	
Command mode	Global configuration mode.	
Usage Guide	This command disables the SNMP agent services of all versions supported on the device.	
Configuration Examples	The following example disables the SNMP agent.	
	FS(config)# no snmp-server	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.3 show snmp

	Use this command to display the SNMP configuration.	
	show snmp [mib user view group host locked-ip process-mib-time]	
Parameter Description	Parameter	Description
	mib	Displays the SNMP MIBs supported.
	user	Displays the SNMP user information.
	view	Displays the SNMP view information.
	group	Displays the SNMP user group information.
	host	Displays the explicit host configuration.
	locked-ip	Displays the source IP addresses locked after continuous SNMP authentication failures.
	process-mib-time	Displays the MIB node requiring the longest processing time.
Defaults	N/A	

Command mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The example below displays the SNMP configuration: <pre> FS# show snmp Chassis: 60FF60 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP global trap: disabled SNMP logging: disabled SNMP agent: enabled </pre>	
Related Commands	Command	Description
	snmp-server chassis-id	Specifies the SNMP system sequence number.
Platform Description	N/A	

1.4 snmp trap link-status

	Use this command to enable the interface to send link traps. Use the no form of this command to disable the interface to send link traps.
	snmp trap link-status
	no snmp trap link-status

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Sending link traps on the interface is enabled by default. If the interface link status changes, SNMP link traps will be sent.	
Command mode	Interface configuration mode	
Usage Guide	This command can be configured on the Ethernet interface, aggregate ports and SVI interfaces.	
Configuration Examples	The following example disables the interface to send link traps. <pre>FS(config)# interface gigabitEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# no snmp trap link-status</pre> The following example enables the interface to send link traps. <pre>FS(config)# interface gigabitEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# snmp trap link-status</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.5 snmp-server authentication attempt

	Use this command to configure the maximum number of continuous SNMP authentication failures, and specified the action policy for the authentication failure. Use the no form of this command to remove the limit of continuous SNMP authentication failures and the related action policies.	
	snmp-server authentication attempt <i>times</i> exceed { lock lock-time <i>minutes</i> unlock }	
	no snmp-server authentication attempt <i>times</i> exceed { lock lock-time <i>minutes</i> unlock }	
Parameter Description	Parameter	Description
	<i>times</i>	The maximum number of continuous SNMP authentication failures. The range is from 1 to 10.
	exceed	Indicates the action policy in the case that the maximum number of continuous SNMP authentication failures is exceeded.
	lock	Indicates that the source IP address is permanently locked to be authenticated and can be unlocked only by the administrator's manual configuration.

	lock-time <i>minutes</i>	Indicates that the source IP address is locked for a period of time. The <i>minutes</i> indicates the lock time, ranging from 1 to 65,535. The unit is minute.
	unlock	Indicates that no action policy is configured for the authentication failed user, that is, the SNMP authentication for this user is allowed.
Defaults	SNMP attack prevention is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	The IP address of the SNMP authentication failed user is added to the blacklist. When the maximum number of continuous SNMP authentication failures is exceeded, the system will perform the related authentication limit actions according the configured policy.: For the permanently locked IP addresses: The source IP addresses can be authenticated only after the administrator unlock them manually. For the IP addresses locked for a period time: The source IP addresses can be authenticated only after the lock time expires or the administrator unlock them manually. For the unlocked IP addresses: The source IP address can pass the authentication as long as the correct community (for SNMPv1 and SNMPv2) or username (for SNMPv3) is used.	
Configuration Examples	The following example configures the maximum number of continuous SNMP authentication failures to 4, and sets the IP address lock time to 30 seconds. <pre>FS(config)# snmp-server authentication attempt 4 exceed lock-time 30</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.6 snmp-server chassis-id

	Use this command to specify the SNMP chassis ID. Use the no form of this command to restore the default chassis ID.	
	snmp-server chassis-id <i>text</i>	
	no snmp-server chassis-id	
Parameter Description	Parameter	Description
	<i>text</i>	SNMP chassis ID: numerals or characters.
Defaults	The default is 60FF60.	

Command mode	Global configuration mode.	
Usage Guide	The SNMP chassis ID is generally the serial number of the device to facilitate identification. The SNMP chassis ID can be displayed through the show snmp command.	
Configuration Examples	The following example specifies the SNMP chassis ID as 123456: <pre>FS(config)# snmp-server chassis-id 123456</pre>	
Related Commands	Command	Description
	show snmp	Displays the SNMP configuration.
Platform Description	N/A	

1.7 snmp-server community

	Use this command to specify the SNMP community access string. Use the no form of this command to remove the SNMP community access string.	
	snmp-server community [0 7] <i>string</i> [view <i>view-name</i>] [[ro rw] [host <i>ipaddr</i>] [ipv6 <i>ipv6-aclname</i>] [<i>aclnum</i>] [<i>aclname</i>]	
	no snmp-server community [0 7] <i>string</i>	
Parameter Description	Parameter	Description
	0	Indicates that the community string is in plaintext.
	7	Indicates that the community string is in ciphertext.
	<i>string</i>	Community string, which is the communication password between the NMS and the SNMP agent
	<i>view-name</i>	View name
	ro	Indicates that the NMS can only read the variables of the MIB.
	rw	Indicates that the NMS can read and write the variables of the MIB.
	<i>aclnum</i>	Access list number (1 to 199, and 1300 to 2699), which specifies the IPv4 addresses that are permitted to access the MIB.
	<i>aclname</i>	Access list name, which specifies the IPv4 addresses that are permitted to access the MIB.
	<i>ipv6-aclname</i>	IPv6 access list name, which specifies the IPv6 addresses that are permitted to access the MIB.
	<i>ipaddr</i>	Specifies the IP address of the NMS to access the MIB.
Defaults	All communities are read only by default.	
Command	Global configuration mode.	

mode		
Usage Guide	This command is an essential command to enable the SNMP agent function, such as specifying the community attribute and IP addresses of NMS to access the MIB. To disable the SNMP agent function, use the no snmp-server command.	
Configuration Examples	The following example defines a SNMP community access string named public, which can be read-only. <pre>FS(config)# snmp-server community public ro</pre>	
Related Commands	Command	Description
	access-list	Defines an access list.
Platform Description	N/A	

1.8 snmp-server contact

	Use this command to specify the system contact string. Use the no form of this command to remove the system contact string.	
	snmp-server contact <i>text</i>	
	no snmp-server contact	
Parameter Description	Parameter	Description
	<i>text</i>	Defines a system contact string.
Defaults	No system contact string is set by default.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies the SNMP system contract i-net800@i-net.com.cn: FS(config)# snmp-server contact <i>i-net800@i-net.com.cn</i>	
Related Commands	Command	Description
	show snmp-server	Displays the SNMP configuration.
	no snmp-server	Disables the SNMP agent function.
Platform Description	N/A	

1.9 snmp-server enable secret-dictionary-check

	Use this command to enable the secret dictionary check for the community and user fields. Use the no form of this command to disable the secret dictionary check.	
	snmp-server enable secret-dictionary-check	
	no snmp-server enable secret-dictionary-check	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Secret dictionary check for the community and user fields is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	This command must be used together with the password policy command.	
Configuration Examples	The following example enables the secret dictionary check for the community field. <pre>FS(config)# password policy min-size 6 FS(config)# snmp-server enable secret-dictionary-check FS(config)# snmp-server community abc12 % The community(abc12) is a weak community!</pre>	
Related Commands	Command	Description
	snmp-server host	Specifies the SNMP host to send the SNMP trap message.
Platform Description	N/A	

1.10 snmp-server enable traps

	Use this command to enable the SNMP agent to send the SNMP trap message to NMS. Use the no form of this command to disable the SNMP agent to send the SNMP trap message to NMS.	
	snmp-server enable traps [<i>notification-type</i>]	
	no snmp-server enable traps	
Parameter Description	Parameter	Description
	<i>notification-type</i>	Specifies the type of trap messages. snmp: SNMP trap message bgp: BGP trap message.

	bridge: Bridge trap message. isis: ISIS trap message. mac-notification: MAC trap message. ospf: OSPF trap message. urpf: uRPF trap message. vrrp: VRRP trap message. web-auth: Web authentication trap message.	
Defaults	Sending trap message to the NMS is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	This command must be used together with the snmp-server host command to send the trap message. Specifying no trap type indicates all trap messages are sent.	
Configuration Examples	The following example enables the SNMP agent to send the SNMP trap message. <pre>FS(config)# snmp-server enable traps snmp FS(config)# snmp-server host 192.168.12.219 public snmp</pre>	
Related Commands	Command	Description
	snmp-server host	Specifies the SNMP host to send the SNMP trap message.
Platform Description	N/A	

1.11 snmp-server flow-control

	Use this command to configure the SNMP flow control. Use the no form of this command to restore the default setting.	
	snmp-server flow-control pps [count]	
	no snmp-server flow-control pps	
Parameter Description	Parameter	Description
	<i>count</i>	Indicates the number of SNMP requests processed per second, ranging from 50 to 65,535.
Defaults	The default count is 300.	
Command mode	Global configuration mode.	

Usage Guide	N/A	
Configuration Examples	The following example configures the number of SNMP requests processed per second to 200. <pre>FS(config)# snmp-server flow-control pps 200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.12 snmp-server group

	Use this command to configure a new SNMP group. Use the no form of this command to remove a specified SNMP group.	
	snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv } } [read <i>readview</i>] [write <i>writeview</i>] [access { [ipv6 <i>ipv6_aclname</i> <i>aclnum</i> <i>aclname</i> } }]	
	no snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv } }	
Parameter Description	Parameter	Description
	v1 v2c v3	Specifies the SNMP version
	auth	Specifies authentication of a packet without encrypting it. This applies to SNMPv3 only.
	noauth	Specifies no authentication a packet. This applies to SNMPv3 only.
	priv	Specifies authentication of a packet with encryption. This applies to SNMPv3 only.
	<i>readview</i>	Specifies a read-only view for the SNMP group. This view enables you to view only the contents of the agent.
	<i>writeview</i>	Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
	<i>aclnum</i>	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
	<i>aclname</i>	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
	<i>ipv6_aclname</i>	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.
Defaults	No SNMP groups are configured by default.	
Command mode	Global configuration mode.	

Usage Guide	N/A	
Configuration Examples	The following example configures a new SNMP group. FS(config)# snmp-server group mib2user v3 priv read mib2	
Related Commands	Command	Description
	show snmp group	Displays the SNMP group configuration.
Platform Description	N/A	

1.13 snmp-server host

	Use this command to specify the SNMP host (NMS) to send the trap message. Use the no form of this command to remove the specified SNMP host.	
	snmp-server host [oob] { <i>host-addr</i> ipv6 <i>ipv6-addr</i> } [vrf <i>vrfname</i>] [traps informs] [version { 1 2c 3 [auth noauth priv]] <i>community-string</i> [udp-port <i>port-num</i>] [via <i>mgmt-name</i>] [<i>notification-type</i>]	
	no snmp-server host [oob] { <i>host-addr</i> ipv6 <i>ipv6-addr</i> } [vrf <i>vrfname</i>] [traps informs] [version { 1 2c 3 [auth noauth priv]] <i>community-string</i> [udp-port <i>port-num</i>] [via <i>mgmt-name</i>]	
Parameter Description	Parameter	Description
	oob	Indicates the out of band communication, that is, the trap messages are sent to the alarm server through the MGMT port. This option is available only when the device is equipped with the MGMT port.
	<i>host-addr</i>	SNMP host address
	<i>ipv6-addr</i>	SNMP host address(ipv6)
	<i>vrfname</i>	Set the name of vrf forwarding table
	trap informs	Enables the host to send the SNMP notification as traps or informs.
	version	SNMP version: V1, V2C or V3
	auth noauth priv	Security level of SNMPv3 users
	<i>community-string</i>	Community string or username (SNMPv3 version)
	<i>port-num</i>	Port of the SNMP host
	via <i>mgmt-name</i>	Specifies the MGMT port.
	<i>notification-type</i>	The type of the SNMP trap message, such as snmp . If no type of the SNMP trap message is specified, all types of the SNMP trap message will be included.
Defaults	No SNMP host is specified by default.	
Command mode	Global configuration mode.	

Usage Guide	This command must be used together with the snmp-server enable traps command to send the SNMP trap messages to NMS. Multiple SNMP hosts can be configured to receive the SNMP trap messages. One host can use different combinations of the types of the SNMP trap message, but the last configuration for the same host will overwrite the previous configurations. In other words, to send different SNMP trap messages to the same host, different combination of SNMP trap messages can be configured. The via parameter can take effect only when the oob parameter is configured. The vrf parameter cannot be used together with the oob parameter.	
Configuration Examples	The following example specifies an SNMP host to receive the SNMP event trap: <pre>FS(config)# snmp-server host 192.168.12.219 public snmp</pre>	
Related Commands	Command	Description
	snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message.
Platform Description	N/A	

1.14 snmp-server inform

	Use this command to configure the resend times for inform requests and the inform request timeout. Use the no form of this command to restore the default settings.	
	snmp-server inform [retries <i>retry-time</i> timeout <i>time</i>]	
	no snmp-server inform	
Parameter Description	Parameter	Description
	<i>retry-num</i>	Specifies the resend times for inform requests, ranging from 0 to 255.
	<i>time</i>	Specifies the inform request timeout, ranging from 0 to 21,474,836.
Defaults	The default <i>retry-num</i> is 3, and the default timeout <i>time</i> is 15 seconds.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the resend times of inform requests to 5. FS(config)# snmp-server inform retries 5 The following example configures the inform request timeout to 20 seconds.	

	FS(config)# snmp-server inform timeout 20	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.15 snmp-server location

	Use this command to set the system location string. Use the no form of this command to remove the system location string.	
	snmp-server location <i>text</i>	
	no snmp-server location	
Parameter Description	Parameter	Description
	<i>text</i>	String that describes the system location information.
Defaults	No system location string is set by default.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the system location information: FS(config)# snmp-server location start-technology-city 4F of A Buliding	
Related Commands	Command	Description
	snmp-server contact	Sets the system contact information.
Platform Description	N/A	

1.16 snmp-server logging

	Use this command to enable the system to log the GET, GET-NETX and SET operations of NMS. Use the no form of this command to disable the SNMP logging function.	
	snmp-server logging { get-operation set-operation }	
	no snmp-server logging { get-operation set-operation }	

Parameter Description	Parameter	Description
	get-operation	Logging function for the GET and GET-NEXT operations.
	set-operation	Logging function for the SET operation.
Defaults	The SNMP logging function is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	This command is used to enable the logging function for the GET, GET-NETX and SET operations of NMS. With the get-operation enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID during the GET and GET-NEXT operations. With the set-operation enabled, the SNMP agent logs the IP address of NMS, operation type and operation node OID and related values during the SET operation. A larger number of logs may affect the device performance. Under normal condition, it is recommended to disable the SNMP logging function.	
Configuration Examples	The following example enables the logging function for the GET and SET operations: <pre>FS(config)#snmp-server logging get-operation FS(config)#snmp-server logging set-operation</pre> The operation logs are displayed as below: <pre>FS#*Feb 7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7) operation(GET) object(id=1.3.6.1.2.1.1.5.0) FS#*Feb 7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7) operation(GET-NEXT) object(id=1.3.6.1.2.1.1.5.0) FS#*Feb 7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7) operation(SET) object(id=1.3.6.1.2.1.1.5.0, value=FS)</pre> The following example disables the logging function for the GET and SET operations: <pre>FS(config)#no snmp-server logging get-operation FS(config)#no snmp-server logging set-operation</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.17 snmp-server net-id

	Use this command to configure the network element coding information of the device. Use the no form of this command to remove the network element coding information.	
	snmp-server net-id <i>text</i>	
	no snmp-server net-id	
Parameter Description	Parameter	Description
	<i>text</i>	Configures the network element coding information of the device. The text length ranges from 1 to 255. The text is case-sensitive, and may contain spaces.
Defaults	No network element coding information is configured by default.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the network element coding text to FZ_CDMA_MSC1.	
	FS(config)# snmp-server net-id FZ_CDMA_MSC1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.18 snmp-server packetsize

	Use this command to specify the largest size of the SNMP packet. Use the no form of this command to restore the default value.	
	snmp-server packetsize <i>byte-count</i>	
	no snmp-server packetsize	
Parameter Description	Parameter	Description
	<i>byte-count</i>	Packet size. The range is from 484 to 17,876 bytes
Defaults	The default is 1,472 bytes.	
Command mode	Global configuration mode.	

Usage Guide	The following example specifies the largest size of SNMP packet as 1,492 bytes: FS(config)# snmp-server packetsize 1492	
Configuration Examples	N/A	
Related Commands	Command	Description
	snmp-server queue-length	Specifies the length of the message queue for each SNMP trap host.
Platform Description	N/A	

1.19 snmp-server queue-length

	Use this command to specify the length of the message queue for each SNMP trap host. Use the no form of this command to restore the default value.	
	snmp-server queue-length <i>length</i>	
	no snmp-server queue-length	
Parameter Description	Parameter	Description
	<i>length</i>	Queue length. The range is from 1 to 1000.
Defaults	The default is 10.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to adjust the length of message queue for each SNMP trap host for the purposes of controlling the speed of sending the SNMP trap messages.	
Configuration Examples	The following example specifies the length of message queue as 100. FS(config)# snmp-server queue-length 100	
Related Commands	Command	Description
	snmp-server packetsize	Specifies the largest size of the SNMP packet.
Platform Description	N/A	

1.20 snmp-server system-shutdown

	Use this command to enable the SNMP message reload function. Use the no form of this command to disable the SNMP message reload function.	
	snmp-server system-shutdown	
	no snmp-server system-shutdown	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The SNMP message reload function is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to enable the SNMP message reload function which may enable the system to send the device reload traps to the NMS before the device is reloaded or rebooted.	
Configuration Examples	The following example enables the SNMP message reload function: <pre>FS(config)# snmp-server system-shutdown</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.21 snmp-server trap-format private

	Use this command to configure the SNMP traps with private fields. Use the no form of this command to restore the default trap format.	
	snmp-server trap-format private	
	no snmp-server trap-format private	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The private field is not carried in the SNMP trap by default.	
Command mode	Global configuration mode.	

Usage Guide	Use this command to configure the SNMP trap format with the private field. Currently, the supported data in the private field is alarm occurrence time. For the specific data type and range of each field, refer to FS-TRAP-FORMAT-MIB.mib file. This command does not work if the traps are sent with SNMPv1.	
Configuration Examples	The following example configures the SNMP trap format with the private field. <pre>FS(config)# snmp-server trap-format private</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.22 snmp-server trap-source

	Use this command to specify the source interface of the SNMP trap message. Use the no form of this command to restore the default value.	
	snmp-server trap-source <i>interface</i>	
	no snmp-server trap-source	
Parameter Description	Parameter	Description
	<i>interface</i>	Specifies the source interface of the SNMP trap messages.
Defaults	By default, the IP address of the interface from which the SNMP packet is sent is just the source address.	
Command mode	Global configuration mode.	
Usage Guide	For easy management and identification, you can use this command to fix a local IP address as the SNMP source address.	
Configuration Examples	The following example specifies the IP address of Ethernet interface 0/1 as the source address of the SNMP trap message: <pre>FS(config)# snmp-server trap-source fastethernet 0/1</pre>	
Related Commands	Command	Description
	snmp-server enable traps	Enables the SNMP agent to send the SNMP trap message to NMS.
	snmp-server host	Specifies the NMS host to send the SNMP trap

		message.
Platform	N/A	
Description		

1.23 snmp-server trap-timeout

	Use this command to define the retransmission timeout time of the SNMP trap message. Use the no form of this command to restore the default value.	
	snmp-server trap-timeout <i>seconds</i>	
	no snmp-server trap-timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout (in seconds) of retransmit the SNMP trap message. The range is from 1 to 1,000.
Defaults	The default is 30 seconds.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies the timeout period as 60 seconds.	
	FS(config)# snmp-server trap-timeout 60	
Related Commands	Command	Description
	snmp-server queue-length	Specifies the length of message queue for the SNMP trap host.
	snmp-server host	Specifies the NMS host to send the SNMP trap message.
	snmp-server trap-source	Specifies the source address of the SNMP trap message.
Platform	N/A	
Description		

1.24 snmp-server udp-port

	Use this command to specify a port to receive SNMP packets. Use the no form of this command to restore the default setting.
	snmp-server udp port <i>port-number</i>

	no snmp-server udp port	
Parameter Description	Parameter	Description
	<i>port-number</i>	Specifies a port to receive the SNMP packets.
Defaults	The default is 161.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies port 15000 to receive the SNMP packets. <pre>FS(config)# snmp-server udp-port 15000</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.25 snmp-server user

	Use this command to configure a new user to an SNMP group. Use the no form of this command to remove a user from an SNMP group.	
	snmp-server user <i>username groupname</i> { v1 v2c v3 [encrypted] [auth { md5 sha } <i>auth-password</i>] [priv des56 <i>priv-password</i>] } [access { [ipv6 <i>ipv6_aclname</i>] [<i>aclnum</i> <i>aclname</i>] }]	
	no snmp-server user <i>username groupname</i> { v1 v2c v3 }	
Parameter Description	Parameter	Description
	<i>username</i>	Name of the user on the host that connects to the agent.
	<i>groupname</i>	Name of the group to which the user belongs.

	v1 v2c v3	Specifies the SNMP version. But only SNMPv3 supports the following security parameters.
	encrypted	Specifies whether the password appears in cipher text. In cipher text format, you need to enter continuous hexadecimal numeric characters. Note that the authentication password of MD5 has a length of 16 bytes, while that of SHA has a length of 20 bytes. Two characters make a byte. The encrypted key can be used only by the local SNMP engine on the switch.
	auth	Specifies which authentication level should be used.
	<i>auth-password</i>	Password string (no more than 32 characters) used by the authentication protocol. The system will change the password to the corresponding authentication key.
	priv	Encryption mode. des56 refers to 56-bit DES encryption protocol. <i>priv-password</i> : password string (no more than 32 characters) used for encryption. The system will change the password to the corresponding encryption key.
	md5	Enables the MD5 authentication protocol. While the sha enables the SHA authentication protocol.
	<i>aclnumber</i>	Access list number, which specifies the IPV4 addresses that are permitted to access the MIB.
	<i>aclname</i>	Name of the access list, which specifies the IPV4 addresses that are permitted to access the MIB.
	<i>ipv6_aclname</i>	Name of the IPv6 access list, which specifies the IPv6 addresses that are permitted to access the MIB.
Defaults	N/A	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures an SNMPv3 user with MD5 authentication and DES encryption: <pre>FS(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr</pre>	
Related Commands	Command	Description
	show snmp user	Displays the SNMP user configuration.
Platform Description	N/A	

1.26 snmp-server view

	Use this command to configure an SNMP view. Use the no form of this command to remove an SNMP view.	
	snmp-server view <i>view-name oid-tree</i> { include exclude }	
	no snmp-server view <i>view-name</i> [<i>oid-tree</i>]	
Parameter Description	Parameter	Description
	<i>view-name</i>	View name
	<i>oid-tree</i>	Specifies the MIB object to associate with the view.
	include	Includes the sub trees of the MIB object in the view.
	exclude	Excludes the sub trees of the MIB object from the view.
Defaults	By default, a view is set to access all MIB objects.	
Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets a view that includes all MIB-2 sub-trees (oid is 1.3.6.1).	
	FS(config)# snmp-server view mib2 1.3.6.1 include	
Related Commands	Command	Description
	show snmp view	Displays the SNMP view configuration.
Platform Description	N/A	

2 RMON Commands

2.1 rmon alarm

	Use this command to monitor a MIB variable. Use the no form of this command to remove the alarm entry. rmon alarm <i>number variable interval {absolute delta } rising-threshold value</i> <i>[event-number] falling-threshold value [event-number] [owner ownername]</i> no rmon alarm <i>number</i>	
Parameter description	Parameter	Description
	<i>number</i>	Alarm number. The value ranges from 1-65,535.
	<i>variable</i>	Alarm variable. The value is a character string consisting of 1 to 255 characters in OID dotted format (the format is entry.integer.instance or a leaf node named .instance, for example. 1.3.6.1.2.1.2.1.10.1).
	<i>interval</i>	Sampling interval. The value ranges from 1 to 2,147,483,647 in the unit of second.
	absolute	Absolute sampling. In this mode, when the sampling time arrives, the system directly invokes the variable value.
	delta	Delta sampling. In this mode, when the sampling time arrives, the system invokes the delta value of the variable within the sampling interval.
	rising-threshold <i>value</i>	Rising threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.
	<i>event-number</i>	The event number ranges from 1 to 65,535.
	falling-threshold <i>value</i>	Falling threshold and the corresponding event number when the threshold is reached. The threshold ranges from -2,147,483,648 to +2,147,483,647.
	owner <i>ownername</i>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
Default	N/A.	
Command mode	Global configuration mode.	
Usage guidelines	The FSOS allows you to modify the configured history information of the Ethernet network, including variable, absolute/delta, owner, rising-threshold/falling-threshold, and the corresponding events. However, the modification does not take effect immediately until the system triggers the monitoring event at the next time.	
Examples	The example below monitors the MIB variable instance ifInNUcastPkts.6. <pre>FS(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner zhangsan</pre>	

Related commands	Command	Description
	rmon event <i>number</i> [log] [trap <i>community</i>] description <i>string</i> [owner <i>owner-string</i>]	Adds an event definition.

2.2 rmon collection history

	Use this command to enable history statistics on the Ethernet interface. Use the no form of this command to remove the history entry. rmon collection history <i>index</i> [owner <i>ownername</i>] [buckets <i>bucket-number</i>] [interval <i>seconds</i>] no rmon collection history <i>index</i>	
Parameter description	Parameter	Description
	<i>index</i>	Index of a history entry. The value ranges from 1 to 65,535.
	owner <i>ownername</i>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
	buckets <i>bucket-number</i>	Capacity of a history entry (that is, the maximum number of history entries). The value ranges from 1 to 65,535. The default value is 10.
	interval <i>seconds</i>	Statistics period. The unit is second. The value ranges from 1 to 3,600. The default value is 1,800 seconds.
Default	N/A.	
Command mode	Interface configuration mode.	
Usage guidelines	The configured history control entry parameters cannot be modified. And the history entry can be removed from the interface where the entry configured.	
Examples	The example below enables log statistics on interface GigabitEthernet 0/1. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface gigabitEthernet 0/1 FS(config-GigabitEthernet0/1)#rmon collection history 1 owner UserA buckets 5 interval 60</pre>	
Related commands	Command	Description
	rmon collection stats <i>index</i> [owner <i>owner-name</i>]	Adds a statistical entry on the Ethernet interface.

2.3 rmon collection stats

	Use this command to monitor an Ethernet interface. Use the no form of this command to remove the configuration. rmon collection stats <i>index</i> [owner <i>owner-string</i>] no rmon collection stats <i>index</i>	

Parameter	Parameter	Description
description	<i>index</i>	Index of the statistic table. The value ranges from 1 to 65,535.
	owner <i>ownername</i>	Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive and do not contain spaces.
Default	N/A.	
Command mode	Interface configuration mode.	
Usage guidelines	N/A.	
Examples	The example below enables monitoring the statistics of interface GigabitEthernet 0/1. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface gigabitEthernet 0/1 FS(config-GigabitEthernet0/1)# rmon collection stats 1 owner UserA</pre>	
Related commands	Command	Description
	rmon collection history <i>index</i> [owner <i>owner-name</i>] [buckets <i>bucket-number</i>] [interval <i>seconds</i>]	Adds a history control entry.

2.4 rmon event

	Use this command to define an event. Use the no form of this command to remove the event entry. <pre>rmon event <i>number</i> [log] [trap <i>community</i>] [description <i>description-string</i>] [owner <i>owner-name</i>]</pre> no rmon event <i>number</i>	
Parameter	Parameter	Description
description	<i>number</i>	Event number. The value ranges from 1 to 65,535.
	log	(Optional) Log event. When a log event is triggered, the system records a log.
	trap <i>community</i>	(Optional) Trap event. When a trap event is triggered, the system sends trap with the group named "community".
	description <i>description-string</i>	(Optional) Description of the event. The value is a character string consisting of 1 to 127 characters.
	owner <i>owner-name</i>	(Optional) Owner of an entry. The value is a character string consisting of 1 to 63 characters that are case sensitive.
Default	N/A.	
Command	Global configuration mode.	

mode		
Usage guidelines	N/A.	
Examples	The example below defines the event actions: log event and send trap message.	
	FS#configure terminal	
	Enter configuration commands, one per line. End with CNTL/Z.	
	FS(config)#rmon event 1 log trap public description "iflnNUcastPkts is abnormal" owner UserA	
Related commands	Command	Description
	rmon alarm number variable interval {absolute delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner ownername]	Adds an alarm entry.

2.5 show rmon

Default	Use this command to display the RMON configuration. show rmo
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	The example below displays the RMON configuration. <pre>FS#show rmon ether statistic table: index = 1 interface = GigabitEthernet 0/1 owner = admin status = 0 dropEvents = 61 octets = 170647461 pkts = 580375 broadcastPkts = 2135 multiPkts = 3615 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0</pre>

```

fragments = 0
jabbers = 0
collisions = 0
packets64Octets = 3254668
packets65To127Octets = 1833370
packets128To255Octets = 2098146
packets256To511Octets = 126716
packets512To1023Octets = 363621
packets1024To1518Octets = 1077865

```

rmon history control table:

```

index = 1
interface = GigabitEthernet 0/1
bucketsRequested = 5
bucketsGranted = 5
interval = 60
owner = UserA
stats = 1

```

rmon history table:

```

index = 1
sampleIndex = 2485
intervalStart = 7d:22h:56m:38s
dropEvents = 0
octets = 5840
pkts = 27
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

```

rmon alarm table:

```

index: 1
interval: 60
oid = 1.3.6.1.2.1.2.2.1.12.6
sampleType: 2
alarmValue: 0
startupAlarm: 3
risingThreshold: 20
fallingThreshold: 10

```

	<pre>risingEventIndex: 1 fallingEventIndex: 1 owner: UserA status: 1 rmon event table: index = 1 description = iflnNUcastPkts is abnormal type = 4 community = public lastTimeSent = 0d:0h:0m:0s owner =UserA status = 1 rmon log table: eventIndex = 1 index = 1 logTime = 6 d:19 h:21 m:48 s logDescription = iflnNUcastPkts is abnormal</pre>					
Related commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					

2.6 show rmon alarm

Default	Use this command to display the RMON alarm table. show rmon alarm
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	The example below displays the RMON alarm table. <pre> FS#show rmon alarm rmon alarm table: index: 1 interval: 60 oid = 1.3.6.1.2.1.2.2.1.12.6 </pre>

	<pre> sampleType: 2 alarmValue: 0 startupAlarm: 3 risingThreshold: 20 fallingThreshold: 10 risingEventIndex: 1 fallingEventIndex: 1 owner: UserA status: 1 </pre>	
Related commands	Command	Description
	rmon alarm <i>number variable</i> <i>interval {absolute delta }</i> rising-threshold <i>value</i> <i>[event-number] falling-threshold value</i> <i>[event-number] [owner</i> <i>ownername]</i>	Adds an alarm entry.

2.7 show rmon event

	Use this command to display the event configuration. show rmon event
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	The example below displays the event configuration. <pre> FS#show rmon event rmon event table: index = 1 description = ifInNUcastPkts is abnormal type = 4 community = public lastTimeSent = 0d:0h:0m:0s owner =UserA status = 1 </pre>

	<pre> rmon log table: eventIndex = 1 index = 1 logTime = 6d:19h:21m:48s logDescription = iflnNUcastPkts is abnormal </pre>	
Related commands	Command	Description
	rmon event <i>number</i> [log] [trap <i>community</i>] [description <i>description-string</i>] [owner <i>ownername</i>]	Adds an event entry.

2.8 show rmon history

	Use this command to display the history information. show rmon history
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	The example below displays the history information. <pre> FS#show rmon history rmon history control table: index = 1 interface = GigabitEthernet 0/1 bucketsRequested = 5 bucketsGranted = 5 interval = 60 owner = UserA stats = 1 rmon history table: index = 1 sampleIndex = 2485 intervalStart = 7d:22h:56m:38s dropEvents = 0 octets = 5840 pkts = 27 broadcastPkts = 0 multiPkts = 0 </pre>

	<pre> crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0 </pre>	
Related commands	Command	Description
	rmon collection history <i>index</i> [owner <i>ownername</i>] [buckets <i>bucket-number</i>] [interval <i>seconds</i>]	Adds a history control entry.

2.9 show rmon statistics

	Use this command to display the RMON statistics. show rmon statistics
Default	N/A.
Command mode	Privileged EXEC mode.
Usage guidelines	N/A.
Examples	The example below displays the RMON statistics. <pre> FS#show rmon statistics ether statistic table: index = 1 interface = GigabitEthernet 0/1 owner = admin status = 0 dropEvents = 61 octets = 170647461 pkts = 580375 broadcastPkts = 2135 multiPkts = 3615 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 </pre>

	<pre>jabbers = 0 collisions = 0 packets64Octets = 3254668 packets65To127Octets = 1833370 packets128To255Octets = 2098146 packets256To511Octets = 126716 packets512To1023Octets = 363621 packets1024To1518Octets = 1077865</pre>	
Related commands	Command	Description
	rmon collection stats <i>index</i> [owner <i>owner-string</i>]	Adds a statistical entry.

3 NTP Commands

3.1 no ntp

	Use this command to disable Network Time Protocol (NTP), and clear all NTP configuration.	
	no ntp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	NTP is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	By default, NTP is disabled. However, once the NTP server or the NTP primary clock is configured, the NTP service will be enabled.	
Configuration Examples	The following example disables NTP.	
	FS(config)# no ntp	
Related Commands	Command	Description
	ntp server	Specifies an NTP server.
Platform Description	N/A	

3.2 ntp access-group

	Use this command to configure an access group to control NTP access. Use the no form of this command to remove the peer access group.	
	ntp access-group { peer serve serve-only query-only } access-list-number access-list-name	
	no ntp access-group { peer serve serve-only query-only } access-list-number access-list-name	
Parameter Description	Parameter	Description
	peer	Allows the device to receive time requests and NTP control queries to synchronize itself to the servers specified in the access list.
	serve	Allows the device to receive time requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.

	serve-only	Allows the device to receive only time requests from the servers specified in the access list.
	query-only	Allows the device to receive only NTP control queries from servers specified in the access list.
	<i>access-list-number</i>	Access control list number, ranging from 1 to 99 and 1300 to 1999.
	<i>access-list-name</i>	Access control list name.
Defaults	No access rule to control NTP access is configured by default, namely, NTP access is granted to all devices.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure an access group to control NTP access, providing a minimal security measures (more secure way is to use the NTP authentication mechanism). The NTP service enables the access group options to be scanned in the following order, from least restrictive to most restrictive: peer, serve, serve-only, query-only. If you do not configure any access groups, NTP access is granted to all devices. However, once you configure the access rule, NTP access is granted only to the devices specified in the access list.  NTP control query is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.	
Configuration Examples	The following example shows how to allow the device to only receive time requests from the device of 192.168.1.1. <pre>FS(config)# access-list 1 permit 192.168.1.1 FS(config)# ntp access-group serve-only 1</pre>	
Related Commands	Command	Description
	ip access-list	Creates an IP access control list.
Platform Description	N/A	

3.3 ntp authenticate

	Use this command to enable NTP authentication. Use the no form of this command to disable NTP authentication.
	ntp authenticate
	no ntp authenticate

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Disabled.	
Command mode	Global configuration mode.	
Usage Guide	If NTP authentication is disabled, the synchronization communication is not encrypted. To enable encrypted communication on the server, enable the NTP authentication and configure other keys globally. NTP authentication is implemented through the trusted key specified by the ntp authentication-key and ntp trusted-key commands.	
Configuration Examples	After an authentication key is configured and specified as the global trusted key, enable NTP authentication. <pre>FS(config)#ntp authentication-key 6 md5 woooooop FS(config)#ntp trusted-key 6 FS(config)#ntp authenticate</pre>	
Related Commands	Command	Description
	ntp authentication-key	Sets the global authentication key.
	ntp trusted-key	Configures the global trusted key.
Platform Description	N/A	

3.4 ntp authentication-key

	Use this command to configure an NTP authentication key. Use the no form of this command to remove the NTP authentication key.	
	ntp authentication-key <i>key-id</i> md5 <i>key-string</i> [<i>enc-type</i>]	
	no ntp authentication-key <i>key-id</i>	
Parameter Description	Parameter	Description
	<i>key-id</i>	Key ID, ranging from 1 to 4294967295.
	<i>key-string</i>	Key string An encrypted key supports up to 64 bytes of length, while a non-encrypted key supports up to 31 bytes.
	<i>enc-type</i>	(Optional) Whether this key is encrypted, where, 0 indicates the key is not encrypted, 7 indicates the key is encrypted simply. The key is not encrypted by default.

Defaults	NTP authentication key is not configured by default.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure an NTP authentication key and enables the md5 algorithm for authentication. Each key presents a unique key ID, which can be configured as a trusted key using the ntp trusted-key command.. You can configure up to 1024 NTP authentication keys. However, each server can support only one key.	
Configuration Examples	The following example configures an NTP authentication key. <pre>FS(config)#ntp authentication-key 6 md5 woooooop</pre>	
Related Commands	Command	Description
	ntp authenticate	Enables NTP authentication.
	ntp trusted-key	Configures an NTP trusted key.
	ntp server	Specifies an NTP server.
Platform Description	N/A	

3.5 ntp disable

	Use this command to disable the device to receive NTP packets on the specified interface.	
	ntp disable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	All NTP packets can be received by default.	
Command mode	Interface configuration mode.	
Usage Guide	The NTP message received on any interface can be provided to the client to carry out the clock adjustment. The function can be set to shield the NTP message received from the corresponding interface. By default, the device receives NTP packets on all interfaces, and adjust clock for the client. You can use this command to disable the device to receive NTP packets on the specified interface.  This command is configured only the interface that can receive and send IP packets.	
Configuration	The following example disables the device to receive the NTP packets.	

Examples	FS(config-if)# no ntp disable	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.6 ntp interval

	Use this command to set the interval for time synchronization between the NTP client and the NTP server. Use the no form of this command to restore the default time synchronization interval. ntp interval <i>seconds</i>	
	no ntp interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the time synchronization interval in seconds. The value ranges from 10 to 2,592,000.
Defaults	The default value is 64.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	 The configuration does not take effect immediately. For immediate validation, enable NTP and then set the interval. If the NTP client has never synchronized the time successfully, it rapidly synchronizes the time at an interval of 5s. Then, it synchronizes time at the preset interval after the first successful time synchronization.	
Configuration Examples	The following example configures the NTP time synchronization interval to 3,600 seconds. FS(config)# ntp interval 3600	

3.7 ntp master

	Use this command to configure the device to act as an authoritative NTP server, synchronizing time to other devices. Use the no form of this command to remove the device as an authoritative NTP server.	
	ntp master [<i>stratum</i>]	
	no ntp master	

Parameter Description	Parameter	Description
	<i>stratum</i>	Stratum level. The range is from 1 to 15. The default is 8.
Defaults	N/A	
Command mode	Global configuration mode.	
Usage Guide	In general, the local device synchronizes time from the external time source directly or indirectly. However, if the time synchronization fails due to network connection trouble, you can use this command to configure the local device to act as an authoritative NTP server to synchronize time to other devices. Once configured, the device will not perform time synchronization with the time source which is of a higher stratum.  Configuring the device to act as an authoritative NTP server (in particular, specify a lower stratum level), may be likely to overwrite the effective time. If multiple devices in the same network are configured with this command, the time synchronization may be instable due to the time difference between the devices.  Before configuring this command, you need to manually correct the system clock to avoid too much bias if the device has never performed time synchronization with the external clock source.	
Configuration Examples	The following example configures the device to act as an authoritative NTP server, and sets the stratum level to 12: <pre>FS(config)# ntp master 12</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 ntp server

	Use this command to specify a NTP server for the NTP client. Use the no form of this command to delete the specified NTP server.	
	ntp server [oob vrf <i>vrf-name</i>] { <i>ip-addr</i> <i>domain</i> ip <i>domain</i> ipv6 <i>domain</i> } [version <i>version</i>] [source <i>if-name</i>] [key <i>keyid</i>] [prefer] [via <i>mgmt-name</i>]	
	no ntp server <i>ip-addr</i>	
Parameter Description	Parameter	Description
	oob	(Optional) Accesses the NTP server from the MGMT interface. By default, this option is disabled.
	vrf <i>vrf-name</i>	Specifies the virtual routing and forwarding (VRF) name. By default, this

		parameter is disabled.
	<i>ip-addr</i>	Sets the IP address of the NTP server. The address can be in IPv4 or IPv6 format.
	<i>domain</i>	Sets the domain name of the NTP server, supporting IPv4 and IPv6.
	<i>version</i>	(Optional) Specifies the NTP version (1-3). The default is NTPv3.
	<i>if-name</i>	(Optional) Specifies the source interface from which the NTP message is sent (L3 interface).
	<i>keyid</i>	(Optional) Specifies the encryption key adopted when communication with the corresponding server. The key ID range is from 1 to 4,294,967,295.
	prefer	(Optional) Specifies the given NTP server as the preferred one.
	<i>mgmt-name</i>	(Optional) Specifies the egress MGMT interface for the packets in oob mode.
Defaults	No NTP server is configured by default.	
Command mode	Global configuration mode.	
Usage Guide	At present, FSOS system only supports clients other than servers. Up to 20 servers can be synchronized. To carry out the encrypted communication with the server, set the global encryption key and global trusted key firstly, and then specify the corresponding key as the trusted key of the server to launch the encrypted communication of the server. It requires the server presents identical global encryption key and global trust key to complete the encrypted communication with the server. In the same condition (for instance, precision), the prefer clock is used for synchronization.  The source interface of NTP packets must be configured with the IP address and can be communicated with the peer.	
Configuration Examples	The following example configures an NTP server. For IPv4: <code>FS(config)# ntp server 192.168.210.222</code> For IPv6: <code>FS(config)# ntp server 10::2</code>	
Related Commands	Command	Description
	no ntp	Disables NTP.
Platform Description	N/A	

3.9 ntp trusted-key

	Use this command to set a global trusted key. Use the no form of this command to remove the global trusted key.
	ntp trusted-key <i>key-id</i>
	no ntp trusted-key <i>key-id</i>

Parameter Description	Parameter	Description
	<i>key-id</i>	Global trusted key ID, ranging from 1 to 4294967295.
Defaults	N/A	
Command mode	Global configuration mode.	
Usage Guide	The NTP communication parties must use the same trusted key. The key is identified by ID and is not transmitted to improve security.	
Configuration Examples	The following example configures an authentication key and sets it as a trusted key. <pre>FS(config)#ntp authentication-key 6 md5 woooooop FS(config)#ntp trusted-key 6 FS(config)#ntp server 192.168.210.222 key 6</pre>	
Related Commands	Command	Description
	ntp authenticate	Enables NTP authentication.
	ntp authentication-key	Configures an NTP authentication key.
	ntp server	Configures an NTP server.
Platform Description	N/A	

3.10 ntp update-calendar

	Use this command to enable the NTP client to periodically update the device clock with the time synchronized from the external source clock. Use the no form of this command to remove this function.	
	ntp update-calendar	
	no ntp update-calendar	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, update the calendar periodically is not configured.	
Command mode	Global configuration mode.	
Usage Guide	By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable	

	this function for keeping the accurate calendar.	
Configuration Examples	The following example configures the NTP update calendar periodically.	
	FS(config)# ntp update-calendar	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.11 show ntp server

	Use this command to display the NTP server configuration.	
	show ntp server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the NTP server.	
	<pre> FS# show ntp server ntp-server source keyid prefer version ----- 10::2 None None FALSE 3 192.168.210.222 None None FALSE 3 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.12 show ntp status

	Use this command to display the NTP configuration.	
	show ntp status	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, VLAN configuration mode	
Usage Guide	Use this command to display the NTP configuration. No configuration is displayed before the synchronization server is configured for the first time.	
Configuration Examples	The following example displays the NTP configuration. <pre>FS# show ntp status Clock is synchronized, stratum 8, reference is 127.127.1.1 nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24 reference time is D4BD819B.433892EE (01:27:55.000 UTC) clock offset is 0.00000 sec, root delay is 0.00000 sec root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4 SNTP Commands

4.1 show sntp

	Use this command to display the SNTP configuration.	
	show sntp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults		
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the SNTP configuration. <pre>FS# show sntp SNTP state : Enable SNTP server : 192.168.4.12 SNTP sync interval : 60 Time zone : +8</pre>	
Related Commands	Command	Description
	sntp enable	Enables SNTP.
Platform Description	N/A	

4.2 sntp enable

	Use this command to enable the SNTP function. Use the no form of this command to restore the default value.	
	sntp enable	
	no sntp enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	SNTP is disabled by default.	

Command mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example enables SNTP. <pre>FS(config)# sntp enable</pre>	
Related Commands	Command	Description
	show sntp	Displays the SNTP configuration.
Platform Description	N/A	

4.3 sntp interval

	Use this command to set the interval for the SNTP client to synchronize its clock with the NTP/SNTP server. Use the no form of this command to restore the default synchronization interval.	
	sntp interval <i>seconds</i>	
	no sntp interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Synchronization interval. The unit is second, and the range is from 60 to 65,535.
Defaults	The default synchronization interval is 1,800 seconds.	
Command mode	Global configuration mode.	
Usage Guide	To make the synchronization interval configuration effective, run the sntp enable command.	
Configuration Examples	The following example configures the synchronization interval to 3,600 seconds. <pre>FS(config)# sntp interval 3600</pre>	
Related Commands	Command	Description
	sntp enable	Enables SNTP.
	show sntp	Displays the SNTP configuration.
Platform Description	N/A	

4.4 sntp server

	Use this command to specify an SNTP server. Use the no form of this command to remove the SNTP server.	
	sntp server [oob] { <i>ip-address</i> <i>domain</i> } [via <i>mgmt-name</i>] [source <i>source-ip-address</i>]	
	no sntp server	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address of the SNTP server.
	oob	(Optional) Accesses the SNTP server from the MGMT interface.
	<i>domain</i>	Specifies the domain name of the SNTP server.
	<i>source-ip-address</i>	(Optional) Indicates the specified source IP address.
	<i>mgmt-name</i>	(Optional) Specifies the egress MGMT interface for the packets in oob mode.
Defaults	No SNTP server is configured by default.	
Command mode	Global configuration mode.	
Usage Guide	As SNTP is fully compatible with NTP, the SNTP server can be used as an NTP server in Internet.	
Configuration Examples	The following example specifies an SNTP server in Internet. FS(config)# sntp server 192.168.4.12	
Related Commands	Command	Description
	show sntp	Displays the SNTP configuration.
	sntp enable	Enables SNTP.
Platform Description	N/A	

5 SPAN-RSPAN Commands

5.1 mac-loopback

	Use this command to enable MAC loopback. Use the no form of this command to disable MAC loopback.	
	mac-loopback	
	no mac-loopback	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	MAC loopback is disabled by default.	
Command mode	Interface configuration mode.	
Usage Guide	The MAC loopback feature must be enabled on the interfaces for purposes of local one-to-many mirroring. (Please enable the MAC loopback feature on the down interface, and do not add other configurations to the interface.)	
Configuration Examples	The following example configures a remote VLAN. <pre>FS(config)#vlan 100 FS(config-vlan)#remote-span FS(config-vlan)#exit</pre> The following example configures a session and specifies the mirrored port. <pre>FS(config)#monitor session 1 remote-source FS(config)#monitor session 1 source interface gigabitEthernet 4/1 both</pre> The following example configures the mirroring port, and enables MAC loopback on the port. <pre>FS(config)#monitor session 1 destination remote vlan 100 interface gigabitEthernet 4/2 switch FS(config)#interface gigabitEthernet 4/2 FS(config-if-GigabitEthernet 4/2)#switchport access vlan 100 FS(config-if-GigabitEthernet 4/2)#mac-loopback</pre> The following example adds interfaces GigabitEthernet 4/3-4 to the remote VLAN. <pre>FS(config)#interface range gigabitEthernet 4/3-4 FS(config-if-range)#switchport access vlan 100</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.2 monitor session

	Use this command to configure the SPAN session and specify the source port (monitored port).
	monitor session <i>session-num</i> source interface <i>interface-id</i> [both rx tx]
	Use this command to configure the SPAN session mirroring only the traffic permitted by the access list
	monitor session <i>session-num</i> source interface <i>interface-id</i> rx acl <i>acl-name</i>
	Use this command to configure the SPAN session and specify the destination port (monitoring port).
	monitor session <i>session-num</i> destination interface <i>interface-id</i> [switch]
	Use this command to configure the SPAN session monitoring the CPU packets.
	monitor session <i>session-num</i> source interface <i>interface-id</i> tx cpu
	Use this command to configure the remote SPAN session ID on the source device..
	monitor session <i>session-num</i> remote-source
	Use this command to configure the remote SPAN session ID on the destination device.
	monitor session <i>session-num</i> remote-destination
	Use this command to configure the remote SPAN session and specify the remote SPAN destination VLAN.
	monitor session <i>session-num</i> destination remote vlan <i>remote-vlan-id</i> interface <i>interface-id</i> [switch]
	Use this command to configure the SPAN session and specify the source VLAN to monitor. Note that the source VLAN should not be a remote VLAN.
	monitor session <i>session-num</i> source vlan <i>vlan-id</i> [rx]
	Use this command to limit the SPAN source traffic to specific VLANs.
	monitor session <i>session-num</i> filter vlan <i>vlan-id-list</i>
	Use this command to remove the specified SPAN session, or remove the source port or destination port of the specified SPAN session.
	no monitor session <i>session-num</i> [source interface <i>interface-id</i> destination interface <i>interface-id</i>]
	Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.
	no monitor session <i>session-num</i> [destination remote vlan <i>remote-vlan-id</i> interface <i>interface-id</i>]

	Use this command to remove the specified remote SPAN session, or remove the destination port of the remote SPAN session.	
	default monitor session <i>session-num</i> [destination remote vlan <i>remote-vlan-id</i> interface <i>interface-id</i>]	
	Use this command to remove the specified SPAN session, or remove the source port or destination port of the SPAN session.	
	default monitor session <i>session-num</i> { source interface <i>interface-id</i> destination interface <i>interface-id</i> }	
Parameter Description	Parameter	Description
	<i>session_number</i>	SPAN session number
	<i>interface-id</i>	Interface name
	acl <i>acl-name</i>	Access list name
	<i>remote-vlan-id</i>	Remote VLAN ID
	<i>vlan-id</i>	VLAN ID (remote VLAN excluded)
	<i>vlan-id-list</i>	VLAN list (remote VLAN excluded)
	rx	Monitors the only received traffic.
	tx	Monitors the only transmitted traffic.
	both	Monitors both received and transmitted traffic. This is the default.
	switch	Enables switching on the destination port. Switching function is disabled by default.
	cpu	Monitors the CPU packets. This is disabled by default.
Defaults	Port monitoring is disabled by default.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure SPAN or remote SPAN, and specify the source port or destination port. If the both, rx or tx is not specified for the source port, the both parameter is the default. Configuring an access list for the source port indicates that only the traffic permitted by the access list is monitored. The switch feature is disabled on the destination port. CPU packet monitoring, which is enabled through the cpu parameter, is disabled by default.	
Configuration Examples	The following example configures the source port and destination port of the SPAN session. <pre>FS(config)# monitor session 1 source interface gigabitEthernet 0/1 FS(config)# monitor session 1 destination interface gigabitEthernet 0/2</pre> The following example configures the SPAN session mirroring only the traffic permitted by the access list. <pre>FS(config)# monitor session 3 source interface gigabitEthernet 0/3 rx acl 90</pre>	

The following example configures a remote SPAN session.

```
FS(config)# monitor session 10 remote-source
```

The following example configures the destination port of the remote SPAN session.

```
FS(config)# monitor session 4 destination remote vlan 10 interface gigabitEthernet 0/5
```

The following example configures the source VLAN of the SPAN session.

```
FS(config)# monitor session 1 source vlan 1
```

The following example removes the SPAN session.

```
FS(config)# no monitor session 1
```

The following example removes the source port and destination port of the SPAN session.

```
FS(config)# no monitor session 1 source interface gigabitEthernet 0/18
```

```
FS(config)# no monitor session 1 destination interface gigabitEthernet 0/18
```

The following example configures the SPAN session monitoring only the traffic sent from CPU.

```
FS(config)# monitor session 3 source interface gigabitEthernet 0/3 tx cpu
```

The following example configures the SPAN session monitoring traffic, including the traffic sent from CPU.

```
FS(config)# monitor session 3 source interface gigabitEthernet 0/3 tx cpu
```

```
FS(config)# monitor session 3 source interface gigabitEthernet 0/3 tx
```

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.3 remote-span

	Use this command to configure a remote SPAN VLAN in VLAN configuration mode. Use the no form of this command to disable the remote SPAN VLAN.	
	remote-span	
	no remote-span	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Remote SPAN VLAN is disabled by default.	

Command mode	VLAN configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures a remote SPAN VLAN. FS(config)# vlan 100 FS(config-vlan)# remote-span	
Related Commands	Command	Description
	show vlan	Displays VLAN configuration.
Platform Description	N/A	

5.4 show monitor

	Use this command to display the SPAN configurations.	
	show monitor [session <i>session_number</i>]	
Parameter Description	Parameter	Description
	<i>session_number</i>	Displays the specified SPAN session.
Defaults	N/A	
Command mode	Privileged EXEC mode, global configuration mode and interface configuration mode	
Usage Guide	N/A	
Configuration Examples	This following example displays all SPAN sessions. FS(config)# show monitor sess-num: 2 span-type: LOCAL_SPAN src-intf: TenGigabitEthernet 0/5 frame-type Both dest-intf: TenGigabitEthernet 0/6 sess-num: 1 span-type: LOCAL_SPAN src-intf:	

	<pre>TenGigabitEthernet 0/3 frame-type Both dest-intf:</pre>	
	The following example displays SPAN session 1. <pre>FS(config)# show monitor session 1 sess-num: 1 span-type: LOCAL_SPAN src-intf: TenGigabitEthernet 0/3 frame-type Both dest-intf: TenGigabitEthernet 0/4</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6 sFlow Commands

6.1 sflow agent

	Use this command to configure the address of the sFlow Agent. sflow agent { address { ip-address ipv6 ipv6-address } } { interface { interface-name ipv6 interface-name } }	
	Use this command to delete the address of the sFlow Agent. no sflow agent { address interface }	
	Use this command to restore the default setting. default sflow agent { address interface }	
Parameter Description	Parameter	Description
	address	Configures the IP address of the sFlow Agent.
	<i>ip-address</i>	sFlow Agent IPv4 address.
	ipv6 <i>ipv6-address</i>	sFlow Agent IPv6 address.
	interface	Configures the interface of the sFlow Agent.
	<i>interface-name</i>	Interface of IPv4 address.
	ipv6 <i>interface-name</i>	Interface of IPv6 address.
Defaults		
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to configure the Agent IP address field in the output sFlow datagram. The datagram not configured with this field cannot be output. The sFlow Agent address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Agent address, a message indicating configuration failure is displayed. It is recommended that the IP address of the sFlow Agent device be configured as the sFlow Agent address.	
Configuration Examples	The following example configures 192.168.2.1 as the sFlow Agent address. FS(config)# sflow agent address 192.168.2.1	
Verification	Use the show sflow command to display the sFlow configuration.	
Prompt Messages	Prompt an error message when the address is invalid. invalid host address.	

Common Errors	N/A
Platforms	N/A

6.2 sflow collector collector-id destination

	Use this command to configure the address of the sFlow Collector. sflow collector <i>collector-id</i> destination { <i>ip-address</i> ipv6 <i>ipv6_address</i> } <i>udp-port</i> [vrf <i>vrf-name</i>] [description <i>collector-name</i>]	
	Use this command to delete the address of the sFlow Collector. no sflow collector <i>collector-id</i> destination { <i>ip-address</i> ipv6 <i>ipv6_address</i> } <i>udp-port</i> [vrf <i>vrf-name</i>] [description <i>collector-name</i>]	
	Use this command to delete the address of the sFlow Collector. default sflow collector <i>collector-id</i> destination { <i>ip-address</i> ipv6 <i>ipv6_address</i> } <i>udp-port</i> [vrf <i>vrf-name</i>] [description <i>collector-name</i>]	
Parameter Description	Parameter	Description
	<i>collector-id</i>	sFlow Collector ID. The range is from 1 to 2.
	<i>ip-address</i>	sFlow Collector IPv4 address
	ipv6 <i>ipv6-address</i>	sFlow Collector IPv6 address
	<i>udp-port</i>	sFlow Collector listening port number
	vrf <i>vrf-name</i>	VRF instance name. It is not configured by default.
	description <i>collector-name</i>	Description of the sFlow Collector.
Defaults		
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to configure the sFlow Collector address. The sFlow Collector address shall be a host address. When a non-host address (for example, a multicast or broadcast address) is configured as the sFlow Collector address, a message indicating configuration failure is displayed. The sFlow Collector monitors the sFlow datagram on the specified port. When the vrf parameter is configured, the corresponding VRF instance must exist. When you remove the a VRF instance, the sFlow Collector address will be removed if this VRF instance is also configured for an sFlow Collector address.	
Configuration Examples	The following example configures 192.168.1.100 as the address of sFlow Collector 1, 6343 as the port number and vpn 1 as the VRF instance.	

	FS(config)# sflow collector 1 destination 192.168.2.100 6343 vrf vpn1
Verification	Use the show sflow command to display the sFlow Collector.
Prompt Messages	Prompt an error message when the address is invalid. invalid host address. No VPN exists. vpn is not exist
Common Errors	N/A
Platforms	N/A

6.3 sflow collector collector-id max-datagram-size

	Use this command to configure the maximum length of the output sFlow datagram. sflow collector <i>collector-id</i> max-datagram-size <i>datagram-size</i>	
	Use this command to restore the default maximum length of the output sFlow datagram. no sflow collector <i>collector-id</i> max-datagram-size	
	Use this command to restore the default maximum length of the output sFlow datagram. default sflow collector <i>collector-id</i> max-datagram-size	
Parameter Description	Parameter	Description
	<i>collector-id</i>	sFlow Collector ID. The range is from 1 to 2.
	max-datagram-size <i>datagram-size</i>	The maximum length of the output sFlow datagram. The range is from 200 to 9,000.
Defaults	The default maximum length of the output sFlow datagram is 1,400.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example configures 1,000 as the maximum length of the output sFlow datagram for sFlow Collector. FS(config)# sflow collector 1 max-datagram-size 1000	
Verification	Use the show sflow command to display the maximum length of the output sFlow datagram.	

Prompt Messages	N/A
Common Errors	N/A
Platforms	N/A

6.4 sflow counter collector

	Use this command to enable the sFlow Agent to send counter samples to the sFlow Collector. sflow counter collector <i>collector-id</i>	
	Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector. no sflow counter collector	
	Use this command to disable the sFlow Agent to send counter samples to the sFlow Collector. default sflow counter collector	
Parameter Description	Parameter	Description
	<i>collector-id</i>	sFlow Collector ID. The range is from 1 to 2.
Defaults		
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	This command can be used for physical ports, SVI ports and sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.	
Configuration Examples	The following example enables interface TenGigabitEthernet 0/5 to send counter samples to sFlow Collector 2. FS(config-if-TenGigabitEthernet 0/5)# sflow counter collector 2	
Verification	Use the show sflow command to display the sFlow counter sampling configuration.	
Prompt Messages	N/A	
Common Errors	N/A	

Platforms	N/A

6.5 sflow counter interval

	Use this command to configure the sFlow counter sampling interval. sflow counter interval <i>seconds</i>	
	Use this command to restore the default sFlow counter sampling interval. no sflow counter interval	
	Use this command to restore the default sFlow counter sampling interval. default sflow counter interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	sFlow counter sampling interval. The range is form 3 to 2,147,483,647. The unit is second.
Defaults	The default sFlow counter sampling interval is 30 seconds.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to configure the global sFlow counter sampling interval, and sFlow Counter sampling of all interfaces uses this sampling interval.	
Configuration Examples	The following example configures the sFlow counter sampling interval to 60 seconds. FS(config)# sflow counter interval 60	
Verification	Use the show sflow command to display the sFlow counter sampling interval.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.6 sflow enable

	Use this command to enable flow sampling and counter sampling on the interface. sflow enable [ingress egress]	
	Use this command to disable flow sampling and counter sampling on the interface. no sflow enable	
	Use this command to disable flow sampling and counter sampling on the interface. default sflow enable	
Parameter Description	Parameter	Description
	ingress	Enables sFlow sampling in ingress direction.
	egress	Enables sFlow sampling in egress direction.
Defaults	The sFlow sampling function on an interface is disabled by default.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	If the direction parameter is not specified, sampling on both directions are enabled. The SVI ports and sub routed ports support only the ingress parameter. The ACL should be configured and applied on the interface before the flow sampling based on ACL matching is enabled.	
Configuration Examples	The following example enables the sFlow sampling on interface TenGigabitEthernet 0/5. <pre>FS(config-if-TenGigabitEthernet 0/5)# sflow enable</pre>	
Verification	Use the show sflow command to display the status of the sFlow sampling function.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.7 sflow flow collector

	Use this command to enable the sFlow Agent to send flow samples to the sFlow Collector. sflow flow collector <i>collector-id</i>	
	Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector. no sflow flow collector	
	Use this command to disable the sFlow Agent to send flow samples to the sFlow Collector. default sflow flow collector	
Parameter Description	Parameter	Description
	<i>collector-id</i>	sFlow Collector ID. The range is from 1 to 2.
Defaults		
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	This command can be used for physical ports, SVI ports, sub routed ports and aggregate ports. sFlow datagrams can be output only when an IP address is configured for the corresponding sFlow Collector.	
Configuration Examples	The following example enables interface TenGigabitEthernet 0/5 to send flow samples to sFlow Collector 2. FS(config-if-TenGigabitEthernet 0/5)# sflow flow collector 2	
Verification	Use the show sflow command to display the sFlow flow sampling configuration.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.8 sflow flow max-header

	Use this command to configure the maximum length of the packet header copied during flow sampling. sflow flow max-header <i>length</i>
	Use this command to restore the default maximum length of the packet header copied during flow sampling.

	no sflow flow max-header	
	Use this command to restore the default maximum length of the packet header copied during flow sampling. default sflow flow max-header	
Parameter Description	Parameter	Description
	<i>length</i>	Maximum length of the packet header to be copied. The range is from 18 to 256. The unit is byte.
Defaults	The default length is 64 bytes.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	Configure the maximum number of bytes of the packet content copied from the header of the original packet. The copied content is recorded in the generated sample.	
Configuration Examples	The following example sets the maximum length of the packet header copied during sFlow flow sampling to 128 bytes. <pre>FS(config)# sflow flow max-header 128</pre>	
Verification	Use the show sflow command to display the maximum length of the packet header copied during sFlow flow sampling.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.9 sflow sampling-rate

	Use this command to configure the sampling rate of sFlow flow sampling. sflow sampling-rate <i>rate</i>
	Use this command to restore the default the sampling rate of sFlow flow sampling. no sflow sampling-rate
	Use this command to restore the default sampling rate of sFlow flow sampling.

	default sflow sampling-rate	
Parameter Description	Parameter	Description
	<i>rate</i>	Sampling rate of sFlow sampling. One packet is sampled from every <i>n</i> packets (<i>n</i> equals the value of rate). The range is from 4,096 to 65,535.
Defaults	The default sFlow flow sampling rate is 8,192.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to configure the global sampling rate of sFlow flow sampling, and sFlow flow sampling of all interfaces uses this sampling rate.	
Configuration Examples	The following example sets the sFlow flow sampling rate to 4,096. <pre>FS(config)# sflow sampling-rate 4096</pre>	
Verification	Use the show sflow command to display the sFlow flow sampling rate.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.10 sflow source

	Use this command to configure the source address of the output packets. sflow source { address { <i>ip-address</i> ipv6 <i>ipv6-address</i> } } { interface { <i>interface-name</i> ipv6 <i>interface-name</i> } }	
	Use this command to remove the source address of the output packets. no sflow source { address interface }	
	Use this command to restore the default source address of the output packets. default sflow source { address interface }	
Parameter Description	Parameter	Description
	address	Configures the source IP address of sFlow output packets
	<i>ip-address</i>	sFlow Source IPv4 address

	ipv6 <i>ipv6-address</i>	sFlow Source IPv6 address
	interface	Configures the source interface of sFlow output packets
	<i>interface-name</i>	sFlow Source interface (configured with an IPv4 address)
	ipv6 <i>interface-name</i>	sFlow Source interface (configured with an IPv6 address)
Defaults	The default sFlow Source address is the local device IP address which is used to ping the destination IP	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to configure the source IP address of the output packets. If a source interface is specified, the primary address of the interface will be the source IP address of the outputs packets. If the source interface is not specified or the IP address of the source interface is unreachable, for example, the interface is shutdown, the default source address will be used.	
Configuration Examples	The following example configures the source address of the sFlow output packets as 192.168.2.1. <pre>FS(config)# sflow source address 192.168.2.1</pre>	
Verification	Use the show sflow command to display the status of the sFlow sampling function.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.11 show sflow

	Use this command to display the sFlow configuration. show sflow	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode/global configuration mode/interface configuration mode	
Default Level	14	

Usage Guide	N/A																														
Configuration Examples	The following example displays the sFlow configuration. <pre> FS(config)#show sflow sFlow datagram version 5 Global information: Agent IP: 10.10.10.10 sflow counter interval:30 sflow flow max-header:64 sflow sampling-rate:8192 Collector information: ID IP Port Size VPN 1 192.168.2.100 6343 1400 2 NULL 0 1400 Port information Interface CID FID Enable TenGigabitEthernet 0/1 0 1 Y TenGigabitEthernet 0/2 0 1 N </pre> Field Description: <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>sFlow datagram version</td><td>sFlow datagram version. Currently, FS supports V5 only.</td></tr> <tr> <td>Agent IP</td><td>IP address of the sFlow Agent. It can be configured by using the sflow Agent address {ip-address ipv6 ipv6-address } command.</td></tr> <tr> <td>sflow counter interval</td><td>Counter sampling interval</td></tr> <tr> <td>sflow flow max-header</td><td>The maximum length of bytes of the packet header to be copied</td></tr> <tr> <td>sflow sampling-rate</td><td>Flow sampling rate</td></tr> <tr> <td>ID</td><td>sFlow Collector ID</td></tr> <tr> <td>IP</td><td>The IP address of the sFlow Collector to receive sFlow datagram</td></tr> <tr> <td>Port</td><td>Port No. of the sFlow Collector to receive sFlow datagram</td></tr> <tr> <td>Size</td><td>The maximum length of the output sFlow datagram</td></tr> <tr> <td>VPN</td><td>VPN instance name of sFlow Collector</td></tr> <tr> <td>Interface</td><td>An interface configured with sFlow function</td></tr> <tr> <td>CID</td><td>The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.</td></tr> <tr> <td>FID</td><td>The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.</td></tr> <tr> <td>Enable</td><td>The status of the sFlow sampling function</td></tr> </table>	Field	Description	sFlow datagram version	sFlow datagram version. Currently, FS supports V5 only.	Agent IP	IP address of the sFlow Agent. It can be configured by using the sflow Agent address {ip-address ipv6 ipv6-address } command.	sflow counter interval	Counter sampling interval	sflow flow max-header	The maximum length of bytes of the packet header to be copied	sflow sampling-rate	Flow sampling rate	ID	sFlow Collector ID	IP	The IP address of the sFlow Collector to receive sFlow datagram	Port	Port No. of the sFlow Collector to receive sFlow datagram	Size	The maximum length of the output sFlow datagram	VPN	VPN instance name of sFlow Collector	Interface	An interface configured with sFlow function	CID	The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.	FID	The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.	Enable	The status of the sFlow sampling function
Field	Description																														
sFlow datagram version	sFlow datagram version. Currently, FS supports V5 only.																														
Agent IP	IP address of the sFlow Agent. It can be configured by using the sflow Agent address {ip-address ipv6 ipv6-address } command.																														
sflow counter interval	Counter sampling interval																														
sflow flow max-header	The maximum length of bytes of the packet header to be copied																														
sflow sampling-rate	Flow sampling rate																														
ID	sFlow Collector ID																														
IP	The IP address of the sFlow Collector to receive sFlow datagram																														
Port	Port No. of the sFlow Collector to receive sFlow datagram																														
Size	The maximum length of the output sFlow datagram																														
VPN	VPN instance name of sFlow Collector																														
Interface	An interface configured with sFlow function																														
CID	The destination sFlow Collector ID to which the sFlow Agent sends the counter samples.																														
FID	The destination sFlow Collector ID to which the sFlow Agent sends the flow samples.																														
Enable	The status of the sFlow sampling function																														
Prompt Messages	N/A																														
Platforms	N/A																														

Reliability Configuration Commands

1 REUP Commands

1.1 link state group

	Use this command to add the port into the specified link state track group. The no form of this command is used to delete a port from the specified link state track group.	
	link state group <i>num</i> { upstream downstream }	
	no link state group	
Parameter Description	Parameter	Description
	<i>num</i>	ID of the link state track group.
	upstream	Configures the port to be an upstream port in the link state track group.
	downstream	Configures the port to be a downstream port in the link state track group.
Defaults	The port is not added into any link state track group.	
Command Mode	Interface configuration mode.	
Usage Guide	First create a link state track group and then add a port into the specified link state track group.	
Configuration Examples	The following example shows how to add the port fa0/2 into the link state track group: <pre>FS(config)# link state track 1 FS(config)# interface fa 0/2 FS(config-if)# link state group 1 upstream</pre>	
Related Commands	Command	Description
	link state track	Enables a link state track group.
Platform Description	N/A.	

1.2 link state track

	Use this command to enable the link state track group. The no form of this command is used to disable a link state track group	
	link state track [<i>num</i> up-delay <i>timer</i>]	
	no link state track [<i>num</i>]	

Parameter Description	Parameter	Description
	<i>num</i>	Interface ID of the link aggregation group.
	up-delay <i>timer</i>	Delay time for link up. By default, there is no delay for link up.
Defaults	N/A.	
Command Mode	Global configuration mode.	
Usage Guide	First create a link state track group and then add a port into the specified link state track group.	
Configuration Examples	The following example shows how to create a link state track group: <pre>FS(config)# link state track 1</pre> The following example shows how to create a link state track group and set the down link to become up after 30s when uplink becomes up: <pre>FS(config)# link state track 1 up-delay 30</pre>	
Related Commands	Command	Description
	link state group	Adds the port to the specified link state track group.
Platform Description	N/A.	

1.3 mac-address-table move update max-update-rate

	Use this command to configure the maximum number of MAC address update packets sent per second.	
	mac-address-table move update max-update-rate <i>pkts-per-second</i>	
	no mac-address-table move update max-update-rate	
Parameter Description	Parameter	Description
	<i>pkts-per-second</i>	The maximum number of MAC address update packets sent per second. It ranges from 0 to 32000, and the default value is 150.
Defaults	A maximum of 150 MAC address update packets are sent per second.	
Command Mode	Global configuration mode.	
Usage Guide	When a link is switched, REUP sends a certain number of MAC address update packets to an uplink device in every	

	second to recover downlink data transmission of the uplink device.	
Configuration Examples	The following example shows how to configure the maximum number of MAC address update packets sent per second: <pre>FS(config)# mac-address-table move update max-update-rate 20</pre>	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

1.4 mac-address-table move update receive

	Use this command to enable REUP to receive the mac-address-table update messages.	
	mac-address-table move update receive	
	no mac-address-table move update receive	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	Disabled.	
Command Mode	Global configuration mode.	
Usage Guide	The dual link backup switchover will lead to the loss of downstream data flow, for the MAC address for the uplink switch has not been updated in time. Therefore, it is necessary to update the MAC address table of the uplink switch, to reduce the loss of L2 data flow. You need to enable the switch of receiving the MAC address update messages on the uplink switch.	
Configuration Examples	<pre>FS(config)# mac-address-table move update receive</pre>	
Related Commands	Command	Description
	mac-address-table move update transit	Enables REUP to transmit the mac-address-table update messages.
Platform Description	N/A.	

1.5 mac-address-table move update receive vlan

	Use this command to configure the VLANs processing MAC address update packets.	
	mac-address-table move update receive vlan <i>vlan-range</i>	
	no mac-address-table move update receive vlan <i>vlan-range</i>	
Parameter Description	Parameter	Description
	<i>vlan-range</i>	Range of the VLANs processing MAC address update packets.
Defaults	All VLANs process MAC address update packets.	
Command Mode	Global configuration mode.	
Usage Guide	This command can be used to disable some VLANs from processing MAC address update packets. VLANs disabled from processing MAC address update packets can still recover downlink data transmission of the uplink device using MAC address update packets, but the capability to provide convergence on link failure will be degraded.	
Configuration Examples	The following example configures VLANs processing MAC address update packets: FS(config)# no mac-address-table move update receive vlan 20	
Related Commands	Command	Description
	mac-address-table move update receive	Enables REUP to receive MAC address update packets.
Platform Description	N/A.	

1.6 mac-address-table move update transit

	Use this command to enable REUP to transmit the mac-address-table update messages.	
	mac-address-table move update transit	
	no mac-address-table move update transit	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	Disabled.	
Command Mode	Global configuration mode.	

Usage Guide	In order to reduce the link switchover and the loss of the downstream data flow, it is necessary to enable the switch of receiving the MAC address update messages on the uplink switch.	
Configuration Examples	FS(config)# mac-address-table move update transit	
Related Commands	Command	Description
	mac-address-table move update transit vlan	Enables REUP to transmit the mac-address-table update messages.
Platform Description	N/A.	

1.7 mac-address-table move update transit vlan

	Use this command to enable REUP to transmit the mac-address update messages.	
	mac-address-table move update transit vlan <i>vid</i>	
	no mac-address-table move update transit vlan	
Parameter Description	Parameter	Description
	<i>vid</i>	ID of the VLAN transmitting MAC address update packets.
Defaults	Transmit the MAC-address update messages in the default VLAN on the port.	
Command Mode	Interface configuration mode.	
Usage Guide	When a link is switched, the VLAN enabled to transmit MAC address update packets will send MAC address update packets to its uplink device.	
Configuration Examples	The following example configures VLANs transmitting MAC address update packets: FS(config)# mac-address-table move update transit	
Related Commands	Command	Description
	mac-address-table move update transit	Enables REUP to receive the mac-address-table update messages.
Platform Description	N/A.	

1.8 mac-address-table update group

	Use this command to set the mac-address-table update group.	
	mac-address-table update group [<i>group-num</i>]	
	no mac-address-table update group	
Parameter Description	Parameter	Description
	<i>group-num</i>	The mac-address-table update group ID.
Defaults	By default, no mac-address-table update group is configured.	
Command Mode	Interface configuration mode.	
Usage Guide	In order to reduce the flood due to the MAC address update and the influence on the normal data transmission of the switch, FS products add a configuration of MAC address update group. Only if all the interfaces are added to a MAC address update group, the downstream data transmission be restored rapidly.	
Configuration Examples	FS(config-if)# mac-address-table update group 2	
Related Commands	Command	Description
	show mac-address-table update group detail	Displays the mac-address-table update group information.
Platform Description	N/A.	

1.9 switchport backup interface interface-id

	Use this command to configure the REUP dual link backup interface.	
	switchport backup interface <i>interface-id</i>	
	no switchport backup	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID of the backup link.
Defaults	N/A.	
Command Mode	Interface configuration mode.	

Usage Guide	Enter the primary interface configuration mode, the interface-id in the parameter is for the backup interface. When the active link fails, the backup link transmission is restored rapidly	
Configuration Examples	The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as primary interface and backup interface: <pre>FS(config)# interface fa 0/1 FS(config-if)# switchport backup interface fa 0/2</pre>	
Related Commands	Command	Description
	show interface switchport backup	Displays the dual link backup configuration on the switch.
Platform Description	N/A.	

1.10 switchport backup interface preemption

	Use this command to configure the REUP link preemption function.	
	switchport backup interface <i>interface-id</i> preemption mode { forced bandwidth off }	
	switchport backup interface <i>interface-id</i> preemption delay <i>delay-time</i>	
	no switchport backup interface <i>interface-id</i> preemption delay	
Parameter Description	Parameter	Description
	<i>interface-id</i>	The interface id of the backup link.
	<i>delay-time</i>	The preemption delay time.
Defaults	The preemption function is disabled by default. The default preemption delay time is 35s.	
Command Mode	Interface configuration mode.	
Usage Guide	The preemption mode includes forced, bandwidth and off. In the bandwidth preemption mode, the interface with high bandwidth has priority over other interfaces to transmit the data. In the forced preemption mode, the primary has priority over backup interfaces to transmit the data. No preemption event occurs in the off preemption mode. By default, the preemption mode is off. The preemption delay refers to the delay time of the link switchover after the restoration of the link failure.	
Configuration Examples	The following example shows how to set the dual link backup, with fa 0/1 and fa 0/2 as the primary interface and backup interface, set the bandwidth preemption mode and 40s preemption delay: <pre>FS(config)# interface fa 0/1</pre>	

	<pre>FS(config-if)# switchport backup interface fa 0/2 preemption mode bandwidth FS(config-if)# switchport backup interface fa 0/2 preemption delay 40</pre>	
Related Commands	Command	Description
	show interface switchport backup	Displays the dual link backup configuration.
Platform Description	N/A.	

1.11 switchport backup interface prefer

	Use this command to configure VLAN load balancing on a link. The no form of this command is used to delete the configured VLAN load strategy.	
	switchport backup interface <i>interface-id</i> prefer instance <i>instance-range</i>	
	no switchport backup interface <i>interface-id</i> prefer	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID of the backup link.
	<i>instance-range</i>	Instance range of loading on the backup interface.
Defaults	No VLAN load on the backup interface.	
Command Mode	Interface configuration mode.	
Usage Guide	MSTP instance mapping can be used to modify the mapping between an instance and a VLAN.	
Configuration Examples	The following example configures VLAN load balancing on dual links. <pre>FS(config)# interface gigabitEthernet 0/1 FS(config-if)# switchport backup interface gigabitEthernet 0/2 prefer instance 1</pre>	
Related Commands	Command	Description
	show interface switchport backup	Displays the configuration of dual-link backup on the switch.
	spanning-tree mst configuration	Configures MSTP instances.
Platform Description	N/A.	

1.12 show interfaces switchport backup

	Use this command to display the dual link backup information on the interfaces.	
	show interfaces [<i>interface-id</i>] switchport backup [<i>detail</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	The interface id of the dual link backup.
	detail	Displays the detailed information about the dual link backup.
Defaults		
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A.	
Configuration Examples	<pre> FS # show interfaces switchport backup detail Switch Backup Interface Pairs: Active Interface Backup Interface State ----- Gi0/23 Gi0/24 Active Up/Backup Standby Interface Pair : Gi0/23, Gi0/24 Preemption Mode : Off Preemption Delay : 35 seconds Bandwidth : Gi0/23(1000 Mbits), Gi0/24(1000 Mbits) </pre>	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

1.13 show link state group

	Use this command to display the information of a link state track group.	
	show link state group	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A.	

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A.	
Configuration Examples	The following example displays the link state track group: <pre> FS # show link state group Link State Group:1 Status: Enabled, UP Upstream Interfaces :Gi0/1(Up) Downstream Interfaces :Gi0/3(Dwn), Gi0/4(Dwn) Link State Group:2 Status: Disabled, Down Upstream Interfaces : Downstream Interfaces : (Up):Interface up (Dwn):Interface Down (Dis):Interface disabled </pre>	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

1.14 show mac-address-table move update

	Use this command to display the statistics about the MAC address updates tranceived on the interface.	
	show mac-address-table move update	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A.	
Configuration Examples	<pre> FS#show mac-address-table move update Mac address table move update status: Transit:disable Receive:disable Max-update-rate:150 Receive vlan:1-4094 </pre>	

	Pair: Ag1,Ag2				
	Members	Status	Transit Count	Transit VLAN	Last Transit Time

	Ag1	Down	0		
	Ag2	Down	0		
	Pair: Ag3,Gi0/6				
	Members	Status	Transit Count	Transit VLAN	Last Transit Time

	Ag3	Down	0		
	Gi0/6	Down	0		
	Pair: Gi0/1,Gi0/2				
	Members	Status	Transit Count	Transit VLAN	Last Transit Time

	Gi0/1	Up	0		
	Gi0/2	Standby	0		
Related Commands	Command				Description
	N/A.			N/A.	
Platform Description	N/A.				

1.15 show mac-address-table update group

	Use this command to display the mac-address-table update group information.	
	show mac-address-table update group [detail]	
Parameter Description	Parameter	Description
	detail	Displays the detailed information about the mac-address-table update group.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A.	
Configuration Examples	FS # configure terminal FS (config)# mac-address-table move update receive FS (config)# interface range gigabitEthernet 0/3-4	

	<pre> FS (config-if-range)# mac-address-table update group FS (config-if-range)# end FS # show mac-address-table update group detail Mac-address-table Update Group:1 Received mac-address-table update message count:7 Group member Receive Count Last Receive Switch-ID Receive Time ----- GigabitEthernet 0/3 0 0000.0000.0000 GigabitEthernet 0/4 0 0000.0000.0000 </pre>	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

1.16 rldp detect-interval

	Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the no form of this command to restore the default value.	
	rldp detect-interval <i>interval</i>	
	no rldp detect-interval	
Parameter Description	Parameter	Description
	<i>interval</i>	Detection interval in the range 2 to 15 seconds
Defaults	3 seconds.	
Command Mode	Global configuration mode.	
Usage Guide	In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.	
Configuration Examples	The following example shows how to set the detection interval as 5s: <pre>FS(config)# rldp detect-interval 5</pre>	
Related Commands	Command	Description
	rldp detect-max	Sets the maximum number of detections.
Platform Description	N/A.	

2 RLDP Commands

2.1 rldp detect-interval

	Use this command to configure the interval at which the RLDP sends the detection message on the port. Use the no form of this command to restore the default value.	
	rldp detect-interval <i>interval</i>	
	no rldp detect-interval	
Parameter Description	Parameter	Description
	<i>interval</i>	Detection interval in the range 2 to 15 seconds
Defaults	3 seconds.	
Command Mode	Global configuration mode.	
Usage Guide	In the environment where STP is enabled, it is recommended that the product of interval multiplying the maximum number of detections is less than the topology convergence time of STP.	
Configuration Examples	The following example shows how to set the detection interval as 5s: FS(config)# rldp detect-interval 5	
Related Commands	Command	Description
	rldp detect-max	Sets the maximum number of detections.
Platform Description	N/A.	

2.2 rldp detect-max

	Use this command to set the maximum number of sending detection packets on the port. If the neighboring port does not respond when this detection number is exceeded, the link is considered faulty. Use the no form of this command to restore it to the default value.	
	rldp detect-max <i>num</i>	
	no rldp detect-max	
Parameter Description	Parameter	Description
	<i>num</i>	Maximum number of detections in the range 2 to 10
Defaults	2.	

Command Mode	Global configuration mode.	
Usage Guide	This command is used together with the detection interval to specify the maximum number of detections.	
Configuration Examples	The following example shows how to set the maximum number of detections as 5: FS(config)# rldp detect-max 5	
Related Commands	Command	Description
	rldp detect-interval	Sets the detection interval.
Platform Description	N/A.	

2.3 rldp enable

	Use this command to enable RLDP globally. Use the no form of this command to disable the function.	
	rldp enable	
	no rldp enable	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	Disabled.	
Command Mode	Global configuration mode.	
Usage Guide	You can enable RLDP on the interface only when the global RLDP is enabled.	
Configuration Examples	The following example shows how to enable RLDP: FS(config)# rldp enable	
Related Commands	Command	Description
	rldp port	Enables the RLDP function on the port.
Platform Description	N/A.	

2.4 rldp neighbor-negotiation

	Use this command to enable RLDP neighbor negotiation. Use the no form or default form of this command to restore the default setting.	
	rldp neighbor-negotiation	
	no rldp neighbor-negotiation	
	default rldp neighbor-negotiation	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	RLDP neighbor negotiation is disabled by default.	
Command Mode	Global configuration mode.	
Usage Guide	With neighbor negotiation enabled, RLDP unidirectional-/bidirectional-link detection starts only after the neighbor negotiation is successful. (Receiving the Prob message from the neighbor indicates the neighbor negotiation is successful.)	
Configuration Examples	The following example shows how to enable RLDP neighbor negotiation: <pre>FS#config FS(config)#rldp neighbor-negotiation</pre>	
Related Commands	Command	Description
	rldp port	Enables the RLDP function on the port.
Platform Description	N/A.	

2.5 rldp port

	Use this command to enable RLDP on the port and specify detection type and troubleshooting method. Use the no form of this command to disable the function.	
	rldp port { unidirection-detect bidirection-detect loop-detect } { warning shutdown-svi shutdown-port block }	
	no rldp port { unidirection-detect bidirection-detect loop-detect }	
Parameter Description	Parameter	Description
	unidirection-detect	Sets unidirectional link detection.
	bidirection-detect	Sets bidirectional link detection.

	loop-detect	Sets loop detection type.
	warning	Warns the user.
	shutdown-svi	Shutowns the SVI the port belongs to.
	shutdown-port	Shutowns the port.
	block	Disables learning and forwarding of a port.
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	The RLDLP detection on the port takes effect only when the global RLDLP is enabled.	
Configuration Examples	The following example shows how to enable the RLDLP detection and specify the failure treatment as block. <pre>FS(config)# interface GigabitEthernet 2/0/9 FS(config-if-GigabitEthernet 2/0/9)# rldp port loop-detect block</pre>	
Related Commands	Command	Description
	rldp enable	Enables RLDLP globally.
Platform Description	N/A.	

2.6 rldp reset

	Use this command to make all the ports that have been handled using rldp shutdown or disable to perform RLDLP detection again.	
	rldp reset	
Parameter Description	Parameter	Description
	N/A.	N/A.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command is used to recover the faulty port. The errdisable recovery can be also used for the purpose. For details, refer to the <i>Configuring Interface</i> chapter.	
Configuration	The example below demonstrates how to use this command:	

Examples	FS# rldp reset	
Related Commands	Command	Description
	rldp enable	Enables RLDP globally.
Platform Description	N/A.	

2.7 show rldp

	Use this command to display the RLDP information.	
	show rldp [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A.	
Configuration Examples	N/A.	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

3 VRRP Commands

3.1 show vrrp

	Use this command to display the VRRP information.	
	show [ipv6] vrrp [brief group]	
Parameter	Parameter	Description
Description	ipv6	(Optional) Applies to IPv6 VRRP.
	brief	(Optional) Displays the brief of the VRRP group.
	<i>group</i>	Number of the VRRP group to be displayed
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	If no optional parameter is used, the information of all VRRP groups is displayed.	
Configuration Examples	The following example displays the information of all VRRP groups. <pre> FS# show vrrp GigabitEthernet 0/0 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec GigabitEthernet 0/0 - Group 2 State is Master Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec </pre>	

	<pre> FS#show ipv6 vrrp GigabitEthernet 0/13 - Group 1 State is Master Virtual IPv6 address is as follows: FE80::2 1::2 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 1 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 100 Master Router is FE80::1 (local), priority is 100 Master Advertisement interval is 1 sec Master Down interval is 3.60 sec </pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
Platform Description	N/A	

3.2 show vrrp interface

	Use this command to display the information of the VRRP on the interface.	
	show [ipv6] vrrp interface <i>type number</i> [brief]	
Parameter Description	Parameter	Description
	ipv6	(Optional) Applies to IPv6 VRRP.
	<i>type</i>	Interface type
	<i>number</i>	Interface number
	brief	(Optional) Displays the brief of the VRRP group on the interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the VRRP information on Ethernet interface E1/0.	
	<pre> FS# show vrrp interface fastethernet 0/0 FastEthernet 0/0 - Group 1 </pre>	

	State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Device is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 9 sec FastEthernet 0/0 - Group 2 State is Master Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Device is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 9 sec	
Related Commands	Command	Description
	vrrp group ip <i>ip address</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device
Platform Description	N/A	

3.3 show vrrp packet statistics

	Use this command to display the statistics of the VRRP packet transmission.	
	show vrrp packet statistics [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and number
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example displays the statistics of VRRP packet transmission on all interfaces.	
	<pre>FS# show vrrp packet statistics Total InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826 OutTransmits: 306079, OutOctets: 7798564 GigabitEthernet 3/0/1 InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657 OutTransmits: 272931, OutOctets: 6675320 GigabitEthernet 3/0/2 InReceives: 0 packets, InOctets: 0, InErrors: 0 OutTransmits: 681, OutOctets: 16344</pre>	
	The following example displays the statistics of VRRP packets on the interface gigabitEthernet 3/0/1.	
	<pre>FS#show vrrp packet statistics gigabitEthernet 3/0/1 GigabitEthernet 3/0/1 InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657 OutTransmits: 273053, OutOctets: 6677760</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.4 vrrp accept_mode

	Use this command to enable the packet accepting function on the IPv6 VRRP virtual router. Use the no form of this command to disable this function.	
	vrrp ipv6 group accept_mode	
	no vrrp ipv6 group accept_mode	
Parameter	Parameter	Description
Description	<i>group</i>	VRRP group number
Defaults	The master IPv6 VRRP is not allowed to accept packets whose destination IPv6 address is the IPv6 address of a virtual router. However, the NA and NS packets should be accepted regardless of the configuration of Accept_Mode. Also, the master IPv6 VRRP virtual router in the owner state will accept and process any packets whose destination IPv6 address is the IPv6 address of a virtual router, regardless of the configuration of Accept_Mode.	
Command Mode	Interface configuration mode	

Usage Guide	Configuration of the network interface is effective for the master virtual router.  Only IPv6 VRRP has this configuration mode.
Configuration Examples	The following example enables the accept mode on the group 1. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 accept_mode </pre>
Platform Description	N/A

3.5 vrrp authentication

	Use this command to enable VRRP authentication. Use the no form of this command to disable this function.	
	vrrp group authentication string	
	no vrrp group authentication	
Parameter		
Description	Parameter	Description
	group	VRRP group number
	string	String for the VRRP group authentication (within 8 bytes, plaintext password)
Defaults	This function is disabled by default. Even if the VRRP function is enabled, no authentication password is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The plain text authentication password cannot guarantee security but only prevents/prompts wrong VRRP configurations. This command is only applicable to VRRPv2 instead of VRRPv3. Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP) packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.	
Configuration Examples	The following example sets the authentication password for VRRP group 1.	
	FS#configure terminal	

	<pre>FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)# vrrp 1 authentication x30dn78k</pre>
Platform	N/A
Description	

3.6 vrrp bfd (Interface Configuration Mode)

	Use this command to enable BFD correlation for the specified IPv4 VRRP group. Use the no form of this command to remove the BFD correlation for the specified IPv4 VRRP group.	
	vrrp group bfd ip-address	
	no vrrp group bfd ip-address	
Parameter	Parameter	Description
Description	group	VRRP group ID
	ip-address	Neighbor IP address
Defaults	By default, no BFD correlation is configured for the IPv4 VRRP group on the interface.	
Command Mode	Interface configuration mode.	
Usage Guide	After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed. The IP address and BFD session of the interface must be configured before configuring the vrrp bfd command.	
Configuration Examples	The following example enables BFD correlation for the VRRP group. On Switch 1: <pre>FS#configure terminal FS(config)#interface vlan 1 FS(config-if-VLAN 1)#ip address 1.1.1.2 255.255.255.0 FS(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3 FS(config-if-VLAN 1)#vrrp 1 ip 1.1.1.1 FS(config-if-VLAN 1)#vrrp 1 bfd 1.1.1.3</pre> On Switch 2: <pre>FS#configure terminal FS(config)#interface vlan 1 FS(config-if-VLAN 1)#ip address 1.1.1.3 255.255.255.0 FS(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3 FS(config-if-VLAN 1)#vrrp 1 ip 1.1.1.1 FS(config-if-VLAN 1)#vrrp 1 bfd 1.1.1.2</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.7 vrrp bfd (Global Configuration Mode)

	Use this command to enable the global BFD correlation for the IPv4 VRRP backup group to detect the master router status. Use the no form of this command to remove the BFD correlation for IPv4 VRRP.	
	vrrp bfd <i>interface-type interface-number ip-address</i>	
	no vrrp bfd	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface type and interface number
	<i>ip-address</i>	Neighbor IP address
Defaults	By default, the global BFD correlation for IPv4 VRRP is disabled.	
Command Mode	Global configuration mode	
Usage Guide	After the global BFD correlation for IPv4 VRRP is configured, the BFD correlation configuration for the IPv4 VRRP groups will be removed. The global BFD correlation for IPv4 VRRP configured later will override the earlier configuration. The IP address and BFD session of the interface must be configured before configuring the vrrp bfd command. The global IPv4 VRRP BFD session applies to the IPv4 VRRP router which consists of two devices only.	
Configuration Examples	The following example enables global BFD correlation for IPv4 VRRP. <pre> FS#configure terminal FS(config)#interface vlan 1 FS(config-if-VLAN 1)#ip address 192.168.201.11 255.255.255.0 FS(config-if-VLAN 1)#bfd interval 50 min_rx 50 multiplier 3 FS(config-if-VLAN 1)#exit FS(config)# vrrp bfd vlan 1 192.168.201.10 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 vrrp delay

	Use this command to set the reload latency of the VRRP group on the interface. Use the no form of this command to restore the default setting.	
	vrrp delay { minimum <i>min-seconds</i> reload <i>reload-seconds</i> }	
	no vrrp delay	
Parameter	Parameter	Description
Description	minimum <i>min-seconds</i>	When the interface is up, VRRP group shall be reloaded after at least min-seconds.
	reload <i>reload-seconds</i>	The reload latency of the VRRP group. If the configured <i>min-seconds</i> is greater than <i>reload-seconds</i> , the actual reload latency of the VRRP group will be min-seconds.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group starts after the delay instead of immediately upon system startup or the interface's resumption, ensuring non-preemption. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP will be started immediately. The two types of delay share a value range of 0 to 60 seconds. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.	
Configuration Examples	The following example sets the VRRP reload latency on E0 to 10 seconds. When E0 is up, VRRP group 1 shall be reloaded in 10 seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#vrrp delay minimum 10 reload 10 FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.9 vrrp description

	Use this command to specify a descriptor for the VRRP.

	Use the no form of this command to restore the default setting.	
	vrrp [ipv6] group description text	
	no vrrp [ipv6] group description	
Parameter	Parameter	Description
Description	ipv6	Applies to IPv6 VRRP.
	<i>group</i>	VRRP group number
	<i>text</i>	VRRP group descriptor
Defaults	This function is disabled by default. Even if the VRRP function is enabled, no VRRP group descriptor is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command will set the descriptor for the VRRP group to facilitate the identification of the VRRP group.	
Configuration Examples	The following example labels the VRRP group 1 on Ethernet interface E0 as Building A – Marketing and Administration. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 description "Building A - Marketing and Administration" FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 fe80::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 description "Building B - Marketing and Administration" </pre>	
Related Commands	Command	Description
	vrrp group ip ip-address [secondary]	Enables the VRRP function and set the IP address for the virtual device
Platform Description	N/A	

3.10 vrrp ip

	Use this command to enable VRRP on the interface and specify the related virtual IP address.	
	Use the no form of this command to restore the default setting.	
	vrrp group ip ipaddress [secondary]	
	no vrrp group ip ipaddress [secondary]	
Parameter	Parameter	Description
Description	<i>group</i>	VRRP group number of the virtual device
	<i>ipaddress</i>	IP address of the virtual device

	secondary	Specifies the secondary IP address of the virtual device.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	If the secondary parameter is not used, the IP address set here will become the master IP address of the virtual device.	
Configuration Examples	The following example enables the VRRP function on Ethernet interface 0. The VRRP group number is 1, primary IP address of the virtual device is 10.0.1.20 and secondary IP address is 10.0.2.20. <pre>FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#ip address 10.0.2.1 255.255.255.0 secondary FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.2.20 secondary</pre>	
Related Commands	Command	Description
	show vrrp [brief group]	Displays the VRRP configuration.
Platform Description	N/A	

3.11 vrrp ipv6

	Use this command to enable IPv6 VRRP on the interface and specify the related virtual IPv6 address. Use the no form of the command to restore the default setting.	
	vrrp group ipv6 <i>ipv6-address</i>	
	no vrrp group ip <i>ipv6-address</i>	
Parameter	Parameter	Description
Description	<i>group</i>	VRRP group number of the virtual device
	<i>ipv6-address</i>	IPv6 address of the virtual device
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	IPv6 VRRP and IPv4 VRRP share group numbers ranging from 1 to 255. One VRRP group number of an interface is applicable to both IPv4 VRRP and IPv6 VRRP at the same time. The first configured address should be the link's	

	local address, which cannot be deleted until the other virtual addresses are deleted.	
Configuration Examples	The following example enables the IPv6 VRRP function on Ethernet interface FastEthernet 0/0 with VRRP group number 1 and virtual IPv6 address FE80::1 and 2001::1. <pre>FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1</pre>	
Related Commands	Command	Description
Commands	show ipv6 vrrp [brief group]	Displays the IPv6 VRRP configuration.
Platform Description	N/A	

3.12 vrrp preempt

	Use this command to set the preemption mode of the VRRP group. Use the no form of this command to restore the default setting.	
	vrrp [ipv6] group preempt [delay seconds]	
	no vrrp [ipv6] group preempt [delay]	
Parameter	Parameter	Description
Description	ipv6	Applies to IPv6 VRRP.
	group	VRRP group number
	delay seconds	(Optional)Specifies the delay before a device declares itself master. The default value is 0.
Defaults	This function is disabled by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.	
Command Mode	Interface configuration mode	
Usage Guide	If the VRRP group is working in the preemption mode, once a device finds its priority is higher than the priority of the master, it will become the master device of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the master's priority, it will not become the master device of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because that VRRP group has the highest priority and thus automatically becomes the master device in the VRRP group.	

Configuration Examples	The following example enables IPv4 VRRP on interface GigabitEthernet 0/0. When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 preempt delay 15 FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 200 </pre> The following example enables IPv4 VRRP on interface GigabitEthernet 0/0. When VRRP group 1 finds its priority (200) is higher than that of the current master device, it will declare its preemption of master after a delay of 15 seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 preempt delay 15 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 200 </pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp group priority <i>level</i>	Sets the VRRP group priority.
Platform Description	N/A	

3.13 vrrp priority

	Use this command to specify the priority of the VRRP group. Use the no form of this command to restore the default setting.	
	vrrp [ipv6] <i>group</i> priority <i>level</i>	
	no vrrp [ipv6] <i>group</i> priority	
Parameter Description	Parameter	Description
	ipv6	Specifies the priority of the IPv6 VRRP group.
	<i>group</i>	VRRP group number
	<i>level</i>	VRRP group priority
Defaults	This function is disabled by default. Once the VRRP function is enabled, the default priority of the VRRP group is	

	100.						
Command Mode	Interface configuration mode						
Usage Guide	This command is used to manually configure the VRRP router priority.						
Configuration Examples	The following example sets the priority of IPv4 VRRP group 1 as 254. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254 </pre> The following example sets the priority of IPv6 VRRP group 1 as 254. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254 </pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>vrrp group ip <i>ipaddress</i> [secondary]</td><td>Enables the VRRP function and set the IP address for the virtual device.</td></tr> <tr> <td>vrrp group preempt [delay seconds]</td><td>Sets the VRRP in the preemption mode.</td></tr> </table>	Command	Description	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.	vrrp group preempt [delay seconds]	Sets the VRRP in the preemption mode.
Command	Description						
vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.						
vrrp group preempt [delay seconds]	Sets the VRRP in the preemption mode.						
Platform Description	N/A						

3.14 vrrp timers advertise

	Use this command to specify the interval for the master device to send the VRRP advertisement. Use the no form of this command to restore the default setting.								
	vrrp [ipv6] group timers advertise { <i>advertise-interval</i> csec <i>centisecond-interval</i> }								
	no vrrp [ipv6] group timers advertise								
Parameter Description	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>ipv6</td><td>Applies to IPv6 VRRP.</td></tr> <tr> <td><i>group</i></td><td>VRRP group number</td></tr> <tr> <td><i>advertise-interval</i></td><td>Sets the interval time in seconds between sending VRRP advertisement.</td></tr> </table>	Parameter	Description	ipv6	Applies to IPv6 VRRP.	<i>group</i>	VRRP group number	<i>advertise-interval</i>	Sets the interval time in seconds between sending VRRP advertisement.
Parameter	Description								
ipv6	Applies to IPv6 VRRP.								
<i>group</i>	VRRP group number								
<i>advertise-interval</i>	Sets the interval time in seconds between sending VRRP advertisement.								

	csec <i>centisecond-interval</i>	Sets the interval time in milliseconds between sending advertisement frames from the master VRRP router in the backup group. The range is from 50 to 99. This value is not set by default. This parameter takes effect only for VRRPv3.
Defaults	This function is disabled by default. Once the VRRP function is enabled, the default advertisement interval of the master device is one second.	
Command Mode	Interface configuration mode	
Usage Guide	If the current device becomes the master device in the VRRP group, it will notify its VRRP status, priority and other information by sending the VRRP advertisement in the set interval. Based on the RFC specification, the maximum advertisement interval of the IPv4/IPv6 VRRPv3 group is 40 seconds. The advertisement interval can be configured larger than 40 seconds, but the effective advertisement interval is 40 seconds.	
Configuration Examples	The following example sets the IPv4 VRRP advertisement interval as 4 seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 4 </pre> The following example sets the IPv6 VRRP advertisement interval as 4 seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise 4 </pre> The following example sets the IPv4 VRRP advertisement interval as 50 centi-seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise csec 50 </pre> The following example sets the IPv6 VRRP advertisement interval as 50 centi-seconds. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. </pre>	

	<pre>FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise csec 50</pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp group timers learn	Enables the timer learning function.
Platform Description	N/A	

3.15 vrrp timers learn

	Use this command to enable the timer learning function. Use the no form of this command to restore the default setting.	
	vrrp [ipv6] group timers learn	
	no vrrp [ipv6] group timers learn	
Parameter Description	Parameter	Description
	ipv6	Applies to IPv6 VRRP.
	<i>group</i>	VRRP group number
Defaults	This function is disabled by default. Even if the VRRP function is enabled, the timer learning function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Once the timer learning function is enabled, if the current device is a VRRP backup device, it will learn the VRRP advertisement interval from the VRRP advertisement of the master device, with which it calculates the master device's failure interval instead of the VRRP advertisement interval configured locally. This command may synchronize the VRRP advertisement timer with the master device.	
Configuration Examples	The following example enables the timer learning function on the IPv4 VRRP group 1. <pre>FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 timers learn</pre>	

	The following example to enables the timer learning function on the IPv6 VRRP group 1. <pre> vrrp ipv6 1 timers learn FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ipv6 enable FS(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1 FS(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers learn </pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp group ipv6 <i>ipaddress</i>	Enables the VRRP function and set the IPv6 address for the virtual device.
	vrrp group timers advertise <i>interval</i>	Sets the IPv4 VRRP advertising interval.
	vrrp ipv6 group timers advertise <i>interval</i>	Sets the IPv6 VRRP advertising interval.
Platform Description	N/A	

3.16 vrrp track

	Use these commands to enable the IPv4/IPv6 VRRP track in the interface configuration mode. Use the no form of these commands to restore the default setting.	
	vrrp group track { <i>interface-type interface-number</i> bfd <i>interface-type interface-number ipv4-address</i> } [<i>priority</i>]	
	vrrp ipv6 group track <i>interface-type interface-number</i> [<i>priority</i>]	
	no vrrp [ipv6] <i>group track interface-type interface-number</i>	
	Use these commands to enable VRRP IPv4/IPv6 address track. Use the no form of these commands to restore the default setting.	
	vrrp group track <i>ipv4-address</i> [interval <i>interval-value</i>] [timeout <i>timeout-value</i>] [retry <i>retry-value</i>] [<i>priority</i>]	
	vrrp ipv6 group track { <i>ipv6-global-address</i> <i>ipv6-linklocal-address interface-type interface-number</i> } [interval <i>interval-value</i>] [timeout <i>timeout-value</i>] [retry <i>retry-value</i>] [<i>priority</i>]	
	no vrrp group track <i>ipv4-address</i>	
	no vrrp ipv6 group track { <i>ipv6-global-address</i> <i>ipv6-linklocal-address interface-type interface-number</i> }	
	Use this command to disable the specified neighbor IP address track via BFD.	
	no vrrp group track bfd <i>interface-type interface-number ipv4-address</i>	
Parameter Description	Parameter	Description
	<i>group</i>	VRRP group number
	<i>interface-type interface-number</i>	Type of monitored interface

	bfd <i>interface-type</i> <i>interface-number ipv4-address</i>	Enables the specified neighbor IP address track via BFD.
	<i>priority</i>	VRRP priority change range when the interface or ip address reachability status changes. If this parameter is not selected, the default value is 10.
	ipv6	Applies to IPv6 VRRP.
	<i>ipv4-address</i>	Monitored IPv4 address. With BFD configured, it refers to the neighbor IP address.
	interval <i>interval-value</i>	The interval of time to probe whether the monitored ip address is reachable or not. If this parameter is not selected, the default value is 3 seconds.
	timeout <i>timeout-value</i>	The timeout time of the unreachable monitored ip address. If this parameter is not selected, the default value is 1 seconds.
	retry <i>retry-value</i>	Track retries. If the value is reached, the link is thought unreachable. If this parameter is not configured, the default value is 3.
	<i>ipv6-global-address</i>	Global unicast IPv6 address
	<i>ipv6-linklocal-address</i>	Local link IPv6 address
Defaults	This function is disabled by default. Even if the VRRP function is enabled, no interface or IP address is specified.	
Command Mode	Interface configuration mode	
Usage Guide	 This command can be used to monitor the outlet links. Note that layer-3 routable logical interfaces can be monitored (such as Routed Port, SVI, Loopback and Tunnel).  If a host is monitored, specify the IPv4 address for the IPv4 VRRP router or the IPv6 address for the IPv6 VRRP router.  If the host IP address is link-local, an interface must be specified.  If a VRRP router owns the IP address of the physical interface, the priority is 255. Keep the priority when the monitored IP address or interface is set.	
Configuration Examples	The following example enables the VRRP group 1 to monitor the routed port Fa1/1. If the Fa1/1 link is disconnected, the priority of the VRRP group decreases by 30. When the Fa1/1 link recovers, the priority of VRRP group 1 is restored. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254 FS(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 1/1 30 </pre>	

	The following example sets the VRRP to track the specified neighbor IP address 192.168.1.3 through BFD: <pre> FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface FastEthernet 0/1 FS(config-if)#no switchport //used on the switch. FS(config-if)#ip address 192.168.1.1 255.255.255.0 FS(config-if)#bfd interval 50 min_rx 50 multiplier 3 FS(config)#interface FastEthernet 0/2 FS(config-if)#no switchport //used on the switch FS(config-if)#ip address 192.168.201.17 255.255.255.0 FS(config-if)#vrrp 1 priority 120 FS(config-if)#vrrp 1 ip 192.168.201.1 FS(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30 FS(config-if)#end </pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp group priority <i>level</i>	Sets the VRRP group priority.
Platform Description	N/A	

3.17 vrrp version

	Use this command to configure the version of sending the IPv4 VRRP multicast packets. For the IPv4 VRRP, there are two versions: VRRPv2 and VRRPv3. Use the no form of this command to restore the default setting.	
	vrrp group version { 2 3 }	
	no vrrp group version	
Parameter Description	Parameter	Description
	2	Uses the VRRPv2 version to send the packets.
	3	Uses the VRRPv3 version to send the packets.
Defaults	The default is VRRPv2.	
Command Mode	Interface configuration mode	
Usage Guide	Considering the compatibility of VRRPv2 and VRRPv3 for the IPv4 VRRP, you can choose the version of VRRP packets based on the actual network environment. VRRPv2 is based on RFC3768 and VRRPv3 is based on RFC 5798.	

	 This command is applicable to IPv4 VRRP only.	
Configuration Examples	The following example configures the version of sending the IPv4 VRRP packets on the interface gi0/0. <pre> FS#configure terminal FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#no switchport //used on the switch. FS(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20 FS(config-if-GigabitEthernet 0/0)# vrrp 1 version 3 </pre>	
Related Commands	Command	Description
	vrrp group ip <i>ipaddress</i> [secondary]	Enables the VRRP function and set the IP address for the virtual device.
	vrrp group timers advertise <i>interval</i>	Sets the interval of sending the VRRP advertisement.
Platform Description	N/A	

3.18 vrrp detection-vlan

	Use this command to enable IPv4 VRRP packets to be sent to only the first or a specified Sub VLAN in a Super VLAN interface. Use the no form of this command to enable IPv4 VRRP packets to be sent to all the Sub VLANs in a Super VLAN interface.	
	vrrp detection-vlan { first-subvlan <i>subvlan-id</i> }	
	no vrrp detection-vlan	
Parameter Description	Parameter	Description
	first-subvlan	IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface.
	<i>subvlan-id</i>	IPv4 VRRP packets are sent to a specified Sub VLAN in a Super VLAN interface.
Defaults	By default, IPv4 VRRP packets are sent to only the first Sub VLAN in a Super VLAN interface.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to configure the mode in which IPv4 VRRP packets are sent to a Super VLAN interface. There are three modes in which IPv4 VRRP packets are sent to a Super VLAN interface: to only the first Sub VLAN, to a specified Sub VLAN, or all Sub VLANs.  This command is configured on a VLAN interface and applies only to Super VLAN interfaces.	

Configuration	The following example enables IPv4 VRRP packets to be sent to all Sub VLANs in Super VLAN 3.	
Examples	<pre>FS#configure terminal FS(config)# vlan 3 FS(config-vlan)# supervlan FS(config-vlan)# subvlan 5-10 FS(config-vlan)#exit FS(config)#interface vlan 3 FS(config-if)# no vrrp detection-vlan</pre>	
Related	Command	Description
Commands	vrrp ip	Enables the VRRP function and set the IP address of the VRRP.
Platform	N/A	
Description		

4 VRRP Plus Commands

4.1 show vrrp balance

	Use this command to display the VRRP Plus brief or details.	
	show vrrp balance [brief <i>group</i>]	
Parameter Description	Parameter	Description
	brief	(Optional) Displays the VRRP Plus brief.
	<i>group</i>	(Optional) Displays the VRRP Plus details.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	If no optional parameter is used, the details of all VRRP Plus group are displayed.	
Configuration Examples	The following example displays the details of all VRRP Plus groups. <pre> FS#show vrrp balance VLAN 1 - Group 1 State is BVG Virtual IP address is 192.168.1.54 Hello time 1 sec, hold time 3 sec Load balancing: host-dependent Redirect time 300 sec, forwarder time-out 14400 sec Weighting 90 (configured 100), thresholds: lower 1, upper 100 </pre>	

```

Track object 1, state: down, decrement weight: 10
There are 2 forwarders
Forwarder 1 (local)
  MAC address:
    0000.5e00.0101
  Owner ID is 00d0.f822.33ab
Forwarder 2
  MAC address:
    001a.a916.0201
Owner ID is 00d0.f822.8800
FS#show ipv6 vrrp balance
VLAN 2 - Group 1
  State is BVG
  Virtual IPv6 address is as follows:
    FE80::8
    2000::8
  Hello time 2 sec, hold time 6 sec
  Load balancing: weighted
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0201
    Owner ID is 00d0.f822.33f5
    Preemption disabled (BVG cannot be preempted)
  Forwarder 2
    MAC address:
      1414.4b72.7701
    Owner ID is 00d0.f822.33b9
Preemption enabled

```

The following example shows the brief of the VRRP Plus group.

```
FS# show vrrp balance brief
```

Interface	Grp	State	Group Addr	MAC addr
VLAN 1	1	BVG	192.168.1.1	0000.5e00.0101

Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.
	vrrp group load-balancing { host-dependent round-robin weighted }	Sets the load balancing policy of the VRRP Plus.
	show vrrp balance interface type number [brief]	Displays the VRRP Plus running status of the specified interface.

Platform	N/A
Description	

4.2 show vrrp balance interface

	Use this command to display the actions of the VRRP Plus group on the specified interface.	
	show vrrp balance interface <i>type number</i> [brief]	
Parameter Description	Parameter	Description
	interface <i>type number</i>	Specifies the interface type and number.
	brief	(Optional) Displays the brief information.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the actions of the VRRP Plus on FastEthernet 0/0. <pre> FS# show vrrp balance interface FastEthernet 0/0 FastEthernet 0/0 - Group 1 State is BVG Virtual IP address is 192.168.1.54 Hello time 1 sec, hold time 3 sec Load balancing: host-dependent Redirect time 300 sec, forwarder time-out 14400 sec Weighting 90 (configured 100), thresholds: lower 1, upper 100 Track object 1, state: down, decrement weight: 10 There are 2 forwarders Forwarder 1 (local) MAC address: 0000.5e00.0101 Owner ID is 00d0.f822.33ab Forwarder 2 MAC address: 001a.a916.0201 Owner ID is 00d0.f822.8800 </pre>	
Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.

	vrrp group load-balancing { host-dependent round-robin weighted }	Sets the load balancing policy of the VRRP Plus.
	show vrrp balance interface type number [brief]	Displays the VRRP Plus running status of the specified interface.
Platform Description	N/A	

4.3 vrrp balance

	Use this command to enable the VRRP Plus function. Use the no form of this command to disable this function.	
	vrrp group balance	
	no vrrp group balance	
Parameter Description	Parameter	Description
	<i>group</i>	Enables the VRRP Plus function on the VRRP of specified group ID.
Defaults	VRRP Plus is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	To enable VRRP Plus, you must configure the VRRP group first.	
Configuration Examples	The following example enables the VRRP Plus function on the Layer 3 interface GigabitEthernet0/0. <pre> FS#config FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.1.1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 balance </pre>	
Related Commands	Command	Description
	vrrp load-balancing	Sets the load balancing policy of the VRRP Plus.
	show vrrp balance	Displays the VRRP Plus running status.
	show vrrp balance interface	Displays the VRRP Plus running status of the specified interface.
Platform Description	N/A	

4.4 vrrp forwarder preempt

	Use this command to enable the forwarding preemption on the VRRP Plus backup group. Use the no form of this command to disable this function.	
	vrrp group forwarder preempt	
	no vrrp group forwarder preempt	
Parameter Description	Parameter	Description
	<i>group</i>	VRRP group number. The range is from 1 to 255.
Defaults	By default, forwarding preemption is enabled.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the forwarding preemption function of the VRRP Plus backup group on the Layer3 interface GigabitEthernet 0/0. <pre> FS#config FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#vrrp 1 ip 192.168.1.1 FS(config-if-GigabitEthernet 0/0)#vrrp 1 balance FS(config-if-GigabitEthernet 0/0)#vrrp 1 forwarder preempt </pre>	
Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.
	show vrrp balance [brief group]	Displays the VRRP Plus running status.
	show vrrp balance interface type number [brief]	Displays the VRRP Plus running status of the specified interface.
Platform Description	N/A	

4.5 vrrp load-balancing

	Use this command to set the VRRP Plus load balancing policy. Use the no form of this command to restore the default setting.	
	Vrrp group load-balancing { host-dependent round-robin weighted } no vrrp group load-balancing { host-dependent round-robin weighted }	

Parameter Description	Parameter	Description
	<i>group</i>	Specifies the VRRP group ID.
	host-dependent	Sets the host-dependent load balancing policy, so as to use the different virtual MACs to reply the host's ARP request based on different hosts.
	round-robin	Sets the round-robin balancing policy, so as to use the different virtual MACs to reply the host's ARP request in turn, which is the default setting.
	weighted	Sets the weight balancing policy, so as to perform the ARP reply based on the device weight of the backup group.
Defaults	The default is round-robin.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the load balancing policy of the VRRP Plus group1 on Layer 3 interface GigabitEthernet0/0 as host-dependent. <pre> FS# config t FS(config)# interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1 FS(config-if-GigabitEthernet 0/0)# vrrp 1 balance FS(config-if-GigabitEthernet 0/0)# vrrp 1 load-balancing host-dependent </pre>	
Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.
	show vrrp balance [brief group]	Displays the VRRP Plus running status.
	show vrrp balance interface type number [brief]	Displays the VRRP Plus running status o the specified interface.
Platform Description	N/A	

4.6 vrrp timers redirect

	Use this command to set the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group. Use the no form of this command to restore the default value.
	vrrp group timers redirect redirect timeout
	no vrrp group timers redirect

Parameter Description	Parameter	Description
	<i>group</i>	VRRP Plus backup group ID, in the range of 1 to 255.
	<i>redirect</i>	The redirection time, 300 seconds (namely 5 minutes) by default, in the range of 0 to 3,600.
	<i>timeout</i>	The timeout, 14,400 seconds (namely 4 hours) by default, in the range of (redirect+600) to 64,800.
Defaults	The default redirection interval is 300 seconds and redirection timeout is 14,400 seconds.	
Command Mode	Interface configuration mode	
Usage Guide	The VRRP Plus function should be enabled before setting the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group.	
Configuration Examples	The following example sets the redirection interval and timeout of the proxy virtual MAC address for the VRRP Plus backup group. <pre> FS#config FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1 FS(config-if-GigabitEthernet 0/0)# vrrp 1 balance FS(config-if-GigabitEthernet 0/0)# vrrp 1 timers redirect 300 6000 </pre>	
Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.
	show vrrp balance [brief group]	Displays the VRRP Plus running status.
	show vrrp balance interface type number [brief]	Displays the VRRP Plus running status o the specified interface.
Platform Description	N/A	

4.7 vrrp weighting

	Use this command to set the weight and threshold of the VRPP Plus backup group. Use the no form of this command to restore the default setting.	
	vrrp group weighting maximum [lower lower] [upper upper]	
	no vrrp group weighting	
Parameter Description	Parameter	Description
	<i>group</i>	VRRP Plus backup group ID, in the range of 1 to 255.

	<i>maximum</i>	Weight, 100 by default, in the range of 2 to 254.
	<i>lower</i>	Weight lower, 1 by default, in the range of 1 to (maximum-1)
	<i>upper</i>	Weight upper, 100 by default, in the range of lower to maximum.
Defaults	VRRP Plus backup group weight: 100 Weight lower: 1 Weight upper: 100	
Command Mode	Interface configuration mode	
Usage Guide	The VRRP Plus function should be enabled before setting the weight and threshold of the VRRP Plus backup group	
Configuration Examples	The following example sets the weight and threshold of the VRRP Plus group1. <pre> FS#config t FS(config)#interface GigabitEthernet 0/0 FS(config-if-GigabitEthernet 0/0)# vrrp 1 ip 192.168.1.1 FS(config-if-GigabitEthernet 0/0)# vrrp 1 balance FS(config-if-GigabitEthernet 0/0)# vrrp 1 weighting 50 lower 30 upper 50 </pre>	
Related Commands	Command	Description
	vrrp group balance	Enables the VRRP Plus function.
	show vrrp balance [brief group]	Displays the VRRP Plus running status.
	show vrrp balance interface <i>type number</i> [brief]	Displays the VRRP Plus running status of the specified interface.
Platform Description	N/A	

5 BFD Commands

5.1 bfd

	Use this command to set the BFD session parameters. Use the no form of this command to remove the setting.	
	bfd interval <i>milliseconds</i> min_rx <i>milliseconds</i> multiplier <i>multiplier-value</i>	
	no bfd interval	
Parameter Description	Parameter	Description
	interval <i>milliseconds</i>	Interval of sending the BFD control messages to the BFD session neighbor. <i>milliseconds</i> : The range is from 50 to 10,000 ms.
	min_rx <i>milliseconds</i>	Expected interval of receiving the BFD control messages from the BFD session neighbor. <i>milliseconds</i> : The range is from 50 to 10,000 ms.
	multiplier <i>multiplier-value</i>	Count of BFD control message not received from the peer in the configured interval. <i>multiplier-value</i> : The range is from 3 to 50.
Defaults	No BFD session parameter is configured by default.	
Command Mode	Interface configuration mode for single-hop sessions, BFD template mode for multi-hop sessions	
Usage Guide	The express forwarding must be enabled before enabling BFD on the routers. BFD session parameters should be consistent on peers, so that associated protocols will take effect at the same time. If not, one-way forwarding will occur. Set the parameters based on interface bandwidth. If interval and min_rx are too short, BFD sessions may occupy much bandwidth and influence data transmission. If multi-hop session parameters need to be configured using a template, configure the template first and then configure BFD multi-hop session parameters.	
Configuration Examples	The following example configures the BFD session parameters on routed port FastEthernet 0/2. <pre>FS(config)# interface fastEthernet 0/2 FS(config)# no switchport FS(config-if)# bfd interval 100 min_rx 100 multiplier 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

5.2 bfd bind peer-ip

	Use this command to create a BFD session to correlate with an interface. Use the no form of this command to remove this setting.	
	bfd bind peer-ip <i>ip-address</i> [source-ip <i>ip-address</i>] process-pst	
	no bfd bind peer-ip <i>ip-address</i>	
Parameter Description	Parameter	Description
	peer-ip <i>ip-address</i>	The peer IP address to be detected, which must be directly connected to the Layer 3 interface.
	source-ip <i>ip-address</i>	Source IP address for sending the BFD packets, which avoids the packets dropped by the URPF in case that this function is used with other functions such the URPF at the same time.
	process-pst	Correlates BFD for the Layer3 interface.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Note that this command must be configured a Layer 3 interface and the peer IP address detected must be the address directly-connected to the interface.	
Configuration Examples	The following example detects the peer 1.1.1.2 through BFD on the routed port to generate the BFD status of the interface. <pre>FS(config)# interface gigabitEthernet 0/2 FS(config-if -GigabitEthernet 0/2)#no sw FS(config-if -GigabitEthernet 0/2)#ip address 1.1.1.1 255.255.255.0 FS(config-if -GigabitEthernet 0/2)#bfd bind peer-ip 1.1.1.2 source-ip 1.1.1.1 process-pst</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.3 bfd cpp

	Use this command to enable the BFD protection policy. Use the no form of this command to disable this function.
	bfd cpp

	no bfd cpp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	BFD protocol is so sensitive that if the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function is valid only for the switches.	
Configuration Examples	The following example enables the BFD protection policy. FS(config)# bfd cpp	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.4 bfd echo

	Use this command to enable echo mode. Use the no form of this command to disable echo mode.	
	bfd echo	
	no bfd echo	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	

Usage Guide	By default, with BFD session parameter configured, the system enables the echo mode automatically. The minimum sending and receiving interval for the echo packets are the values of the configured interval <i>milliseconds</i> and min_rx <i>milliseconds</i>. This command cannot be configured on the AP port. Before enabling BFD echo mode, it is necessary to use the no ip redirects command to disable the ICMP redirection messages sending on the neighbor device of the BFD session, use the no ip deny land to disable the DDOS (Land-based attack prevention) function. With both ends of the BFD session enabled, the echo mode takes effect. In the process that the forwarding plane of the peer device returns echo packets transmitted by the local end to the local end, the echo packets may be lost due to congestion of the peer device, causing a session detection failure. In this case, configure Quality of Service (QoS) policies to ensure that echo packets are processed preferentially or disable the echo function. The echo detection function of BFD does not support multi-hop detection. Ensure that the echo function is disabled when configuring multi-hops.	
Configuration Examples	The following example enables the echo mode on the routed port FastEthernet 0/2: <pre>FS(config)# interface fastEthernet 0/2 FS(config)# no switchport FS(config-if)# bfd echo</pre>	
Related Commands	Command	Description
	bfd	Configures the BFD session parameter.
	bfd slow-timer	Configures the slow-timer time.
Platform Description	N/A	

5.5 bfd slow-timer

	Use this command to set the slow timer, which is used to send the BFD packets in the BFD asynchronous mode. Use the no form of this command to restore the default setting.	
	bfd slow-timer [<i>milliseconds</i>]	
	no bfd slow-timer	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	BFD slow-timer time. The range is from 1,000 to 30,000. The unit is millisecond.
Defaults	The default slow-timer is 2,000 milliseconds.	
Command Mode	Global configuration mode	

Usage Guide	N/A				
Configuration Examples	The following example sets the slow-timer to 14,000 milliseconds. <pre>FS(config)# bfd slow-timer 14000</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>bfd echo</td><td>Enables the BFD echo function</td></tr> </table>	Command	Description	bfd echo	Enables the BFD echo function
Command	Description				
bfd echo	Enables the BFD echo function				
Platform Description	N/A				

5.6 bfd up-dampening

	Use this command to set the BFD up-dampening time. Use the no form of this command to restore the default setting.	
	bfd up-dampening [<i>milliseconds</i>]	
	no bfd up-dampening	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	(Optional) Sets the BFD up-dampening time. The range is from 0 to 300,000. The unit is millisecond.
Defaults	The default is 0 millisecond, which means that the notification is sent to the related application once the session state is UP.	
Command Mode	Interface configuration mode for single-hop sessions, BFD template mode for multi-hop sessions	
Usage Guide	This function needs to be enabled only when the link is instable. If a BFD session does not frequently switch over between Down and Up, the enabling of BFD flapping dampening will delay notifying an associated application of BFD Up. If multi-hop session parameters need to be configured using a template, configure the template first and then configure BFD multi-hop session parameters.	
Configuration Examples	The following example sets the BFD up-dampening time to 60,000 milliseconds. <pre>FS(config)# bfd up-dampening 60000</pre>	
Related Commands	Command	Description
	bfd	Configures the BFD session parameter.

Platform	N/A
Description	

5.7 show bfd neighbors

	Use this command to display the BFD session parameters.	
	show bfd neighbors [vrf <i>vrf-name</i>] [client { ap bgp isis ospf ospfv3 rip vrrp static-route pbr vrrp-balance pst }] [ipv4 <i>ip-address</i> ipv6 <i>ip-address</i>] [details]	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	(Optional) sets the neighbor VRF name.
	client	(Optional) specifies the routing protocol.
	ap	Displays the BFD session configuration for Layer 3 aggregate ports.
	bgp	Displays the BFD session configuration for BGP.
	isis	Displays the BFD session configuration for ISIS.
	ospf	Displays the BFD session configuration for OSPF.
	ospfv3	Displays the BFD session configuration for OSPFv3.
	rip	Displays the BFD session configuration for RIP.
	vrrp	Displays the BFD session configuration for VRRP.
	static-route	Displays the BFD session configuration for the static route.
	pbr	Displays the BFD session configuration for PBR.
	vrrp-balance	Displays the BFD session configuration for the VRPP.
	pst	Displays the BFD session configuration and the Layer3 interface status.
	ipv4 <i>ip-address</i>	(Optional) Displays the session information of the specified IPv4 neighbor.
	ipv6 <i>ip-address</i>	(Optional) Displays the session information of the specified IPv6 neighbor.
	details	(Optional) Displays the configurations in detail.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	In the information displayed by the show bfd neighbors command, the OurAddr field means the source address of the session. The "-" is displayed if the source address is not specified, and it occurs in the BFD session for the LSP backward IP correlation.	
Configuration Examples	The following example displays the BFD session configuration. <pre>FS# sh bfd neighbors IPV4 sessions: 1, UP: 1 IPV6 sessions: 0, UP: 0 OurAddr NeighAddr LD/RD RH Holdown(mult) State Int 192.168.24.2 192.168.24.1 8192/8192 Up 0(3) Up GigabitEthernet 0/1</pre> The following example displays the BFD session configuration in detail.	


```

FS#sh bfd neighbors
IPv4 sessions: 1, UP: 1
IPv6 sessions: 0, UP: 0
OurAddr      NeighAddr    LD/RD      RH/RS      Holdown(mult) State Int
192.168.24.2  192.168.24.1  8192/8192  Up         0(3 )      Up    GigabitEthernet 0/1
Session state is Up and using echo function with 50 ms interval.
Local Diag:  0,      Demand mode:  0,      Poll bit:  0
MinTxInt: 3000000,   MinRxInt: 3000000,   Multiplier:  3
Received MinRxInt 3000000, Multiplier: 3
Holdown (hits): 9000(0), Hello (hits): 3000(36)
Rx Count: 127, Rx Interval (ms) min/max/avg: 40/999/999
Tx Count: 135, Tx Interval (ms) min/max/avg: 1000/1000/999
Registered protocols: VRRP
Uptime: 0:01:19
Last packet:
Version      :      1          - Diagnostic      : 0
State bit    :      Up        - Demand bit     : 0
Poll bit     :      0         - Final bit      : 0
Multiplier   :      3         - Length         : 24
My Discr     :      8192       - Your Discr     : 8192
Min tx interval : 3000000      - Min rx interval: 3000000
Min Echo interval: 50000

```

The following example displays the BFD session configuration for Layer 3 aggregate ports.

```

FS#show bfd neighbors client ap
IPv4 sessions: 1, UP: 0
IPv6 sessions: 0, UP: 0
OurAddr      NeighAddr    LD/RD      RH/RS      Holdown(mult) State Int
192.168.23.1  192.168.23.2  8192/0     Admin      0(3 )      Down  GigabitEthernet 0/2 (AP 1)

```

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6 IP Event Dampening Commands

6.1 dampening

	Use this command to enable the IP event dampening function on the interface. Use the no or default form of this command to disable this function.	
	dampening [<i>half-life-period</i> [<i>reuse-threshold</i> <i>suppress-threshold</i> <i>max-suppress</i> [restart [<i>restart-penalty</i>]]]]	
	no dampening	
	default dampening	
Parameter Description	Parameter	Description
	<i>half-life-period</i>	Configures the half-life period of suppression penalty. The range is from 1 to 30. The unit is seconds. The default value is 5 seconds.
	<i>reuse-threshold</i>	Configures the penalty threshold to unsuppress the interface. The range is from 1 to 20,000. The default value is 1,000.
	<i>suppress-threshold</i>	Configures the penalty threshold to suppress the interface. The range is from 1 to 20,000. The default value is 2,000.
	<i>max-suppress</i>	Configures the maximum suppress time. The range is from 1 to 255. The default value is 4 times of the <i>half-life-period</i> .
	restart-penalty	Configures the initial penalty value on the interface. The range is from 1 to 20,000. The default value is 2,000.
Defaults	IP event dampening is disabled by default.	
Command mode	Interface configuration mode.	
Usage Guide	This function will influence the modules of the directly-connected/host route, static route, dynamic route and VRRP. If one interface meets the configuration condition of this command, which is in the suppression status, the above influenced modules consider the status of this interface as DOWN, so as to delete the corresponding route and not transceive the data packets on this interface. Re-configuring the dampening command on the interface that has been configured this command makes all dampening information on this interface cleared. However, the interface flapping times will be remained unless use the clear counters command to clear the statistical information of the interface.	
Configuration Examples	The following example configures the IP event dampening function. <pre>FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no switchport FS(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100</pre>	

Related Commands	Command	Description
	clear counters	Clears the interface counters.
	show dampening interface	Displays the statistics of the dampening interface.
	show interface dampening	Displays details of the dampening interface.
Platform Description	When a Layer-3 port on a switch is converted to a Layer-2 port (for example, from a routed port to a switch port), the IP Event Dampening configuration on the port will be deleted.	

6.2 show dampening interface

	Use this command to show the statistics of the dampening interface.	
	show dampening interface	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode/ global configuration mode/ interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistics of the dampening interface. <pre>FS# show dampening interface 3 interfaces are configured with dampening. No interface is being suppressed.</pre>	
Related Commands	Command	Description
	dampening	Enables the IP event dampening function on the interface.
	clear counters	Clears the interface counters.
	show interface dampening	Displays details of IP event dampening configuration.
Platform Description	N/A	

6.3 show interface dampening

	Use this command to display the details of IP event dampening configuration.																													
	show interface [<i>interface-id</i>] dampening																													
Parameter Description	Parameter				Description																									
	<i>interface-id</i>				Interface name																									
Defaults	N/A																													
Command mode	Privileged EXEC mode/ global configuration mode/ interface configuration mode																													
Usage Guide	If the interface-id is specified, only the dampening information of this specified interface is displayed.																													
Configuration Examples	The following example shows the details of IP event dampening configuration. FS# show interface dampening Ethernet1/0 <table><tr><td>Flaps</td><td>Penalty</td><td>Supp</td><td>ReuseTm</td><td>HalfL</td><td>ReuseV</td><td>SuppV</td><td>MaxSTm</td><td>MaxP</td><td>Restart</td></tr><tr><td>0</td><td>0</td><td>FALSE</td><td>0</td><td>5</td><td>1000</td><td>2000</td><td>20</td><td>16000</td><td>0</td></tr></table>										Flaps	Penalty	Supp	ReuseTm	HalfL	ReuseV	SuppV	MaxSTm	MaxP	Restart	0	0	FALSE	0	5	1000	2000	20	16000	0
Flaps	Penalty	Supp	ReuseTm	HalfL	ReuseV	SuppV	MaxSTm	MaxP	Restart																					
0	0	FALSE	0	5	1000	2000	20	16000	0																					
	Domain					Description																								
	Flaps					Interface flapping times.																								
	Penalty					The current penalty value on the interface.																								
	Supp					Suppressed or not.																								
	ReuseTm					Time to unsuppress the interface, in seconds.																								
	HalfL					Half-life period, in seconds.																								
	ReuseV					Unsuppressed threshold.																								
	SuppV					Start suppression threshold.																								
	MaxSTm					Maximum suppression time.																								
	MaxP					Maximum penalty value.																								
	Restart					The initial penalty value on the interface.																								
Related Commands	Command					Description																								
	dampening					Enables the IP event dampening function.																								
	clear counters					Clears the interface counters.																								
	show dampening interface					Displays statistics of the dampening interface.																								
Platform Description	N/A																													

7 stacking Commands

7.1 dad relay enable

	Use this command to enable the Dual-Active Detection (DAD) relay function. Use the no form of this command to restore the default setting.	
	dad relay enable	
	no dad relay enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is only supported on the aggregate port (AP).	
Configuration Examples	The following example enables the AP-based DAD relay function. <pre>FS(config)#interface aggregateport 1 FS(config-if-AggregatePort 1)#dad relay enable</pre> The following example disables the AP-based DAD relay function. <pre>FS(config)#interface aggregateport 1 FS(config-if-AggregatePort 1)#no dad relay enable FS(config-if-AggregatePort 1)#exit</pre>	
Related Commands	Command	Description
	dual-active detection	Configures DAD.
	dual-active pair interface	Configures a pair of Bidirectional Forwarding Detection (BFD)-based DAD interfaces.
	dual-active exclude interface	Configures an exclude interface of DAD.
	show switch virtual dual-active	Displays the configuration and status of DAD.
Platform	N/A	
Description		

7.2 dual-active bfd interface

	Use this command to configure a BFD port. Use the no form of this command to remove the setting.
	dual-active bfd interface <i>interface-name</i>
	no dual-active bfd interface <i>interface-name</i>

Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	config-vs-domain configuration mode	
Usage Guide	The BFD port must be a routing port on the peer end.	
Configuration Examples	The following examples configures interface Gi 1/1/1 as a BFD port. <pre> FS(config)# interface GigabitEthernet 1/1/1 FS(config-if- GigabitEthernet 1/1/1)# no switchport FS(config)# interface GigabitEthernet 2/1/1 FS(config-if- GigabitEthernet 2/1/1)# no switchport FS(config)# switch virtual domain 1 FS(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/1 FS(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/1 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.3 dual-active detection

	Use this command to enable DAD. Use the no form of this command to restore the default setting.	
	dual-active detection { bfd aggregateport }	
	no dual-active detection { bfd aggregateport }	
Parameter	Parameter	Description
Description	bfd	BFD-based DAD
	aggregateport	AP-based DAD
Defaults	This function is disabled by default.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	Configure this command only in virtual switch unit (stacking) mode.	
Configuration	The following example enables BFD-based DAD.	

Examples	<pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# dual-active detection bfd</pre>	
	The following example disables BFD-based DAD. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# no dual-active detection bfd</pre>	
	The following example enables AP-based DAD. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# dual-active detection aggregateport</pre>	
	The following example disables AP-based DAD. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)#no dual-active detection aggregateport</pre>	
Related Commands	Command	Description
	dual-active pair interface	Configures a DAD interface.
	dual-active exclude interface	Configures an exclude interface of DAD.
	show switch virtual dual-active	Displays the configuration and status of DAD.
Platform	N/A	
Description		

7.4 dual-active exclude interface

	Use this command to configure an exclude interface of DAD. Use the no form of this command to remove the exclude interface setting.	
	dual-active exclude interface <i>interface-name</i>	
	no dual-active exclude interface <i>interface-name</i>	
Parameter	Parameter	Description
	<i>interface-name</i>	Interface name
Defaults	N/A	
Command Mode	config-vs-domain configuration mode	
Usage Guide	Configure this command only in stacking mode. An exclude interface must be a routing interface instead of a virtual switch link (VSL) interface. Multiple exclude interfaces are supported.	
Configuration Examples	The following example configures interface Gi 1/1/3 as an exclude interface of DAD. <pre>FS(config)# interface GigabitEthernet 1/0/3 FS(config-if- GigabitEthernet 1/0/3)# no switchport</pre>	

	<pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# dual-active exclude interface GigabitEthernet 1/0/3</pre>	
Related Commands	Command	Description
	dual-active detection	Configures DAD.
	dual-active pair interface	Configures a DAD interface.
	show switch virtual dual-active	Displays the configuration and status of DAD.
Platform Description	N/A	

7.5 dual-active interface

	Use this command to configure an AP-based DAD interface. Use the no form of this command to remove the setting.	
	dual-active interface <i>interface-name</i>	
	no dual-active interface	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface type and interface number. An AP-based DAD interface must be specified.
Defaults	N/A	
Command Mode	config-vs-domain configuration mode	
Usage Guide	Only one AP-based detection interface can be configured. Create an AP-based interface before setting it to a detection interface. The previous detection interface will be overwritten by the current detection interface.	
Configuration Examples	The following example configures AP 1 as the AP-based detection interface.	
	<pre>FS(config)# interface aggregateport 1 FS(config-if-AggregatePort 1)#exit FS(config)# switch virtual domain 1 FS(config-vs-domain)# dual-active interface aggregateport 1</pre>	
Related Commands	Command	Description
	dual-active detection	Configures BFD-/AP-based DAD.
	show switch virtual dual-active	Displays the configuration and status of DAD.
Platform Description	N/A	

7.6 port-member interface

	Use this command to add a VSL-AP member interface. Use the no form of this command to delete a VSL-AP member interface.	
	port-member interface <i>interface-name</i>	
	no port-member interface <i>interface-name</i>	
Parameter	Parameter	Description
Description	<i>interface-name</i>	Interface name, for example, GigabitEthernet 0/1 and GigabitEthernet 0/3.
Defaults	N/A	
Command Mode	config-vsl-port configuration mode	
Usage Guide	Configure this command in stacking mode or in standalone mode.	
Configuration Examples	The following example adds and deletes a VSL-AP member port in standalone mode. <pre>FS(config)# vsl-port FS(config-vsl-port)# port-member interface GigabitEthernet 0/1 FS(config-vsl-port)# no port-member interface GigabitEthernet 0/2</pre> The following example adds and deletes a VSL-AP member port in stacking mode. <pre>FS(config)# vsl-port FS(config-vsl-port)# port-member interface GigabitEthernet 1/0/1 FS(config-vsl-port)# no port-member interface GigabitEthernet 1/0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 led-blink

	Use this command to configure LED blink function.	
	led-blink {enable disable} [device <i>device_id</i>]	
Parameter	Parameter	Description
Description	enable	Enables this function.
	disable	Disables this function.
	<i>device_id</i>	Device ID
Defaults	This function is disabled by default.	

Command Mode	Privileged EXEC mode				
Usage Guide	In single-device mode, this function can be only enabled and disabled. In stacking mode, a device can be specified. If not specified, all devices in the stacking will be configured. If running for 30 minutes, this function is disabled automatically even without any operation. The configuration cannot be saved. In case of restart or active/standby switch-over, it will be removed.				
Configuration Examples	The following example enables and disables LED blink function. <pre>FS#led-blink enable FS#led-blink disable</pre> The following example enables and disables LED blink function on Device 2. <pre>FS#led-blink enable device 2 FS#led-blink disable device 2</pre> The following example enables and disables LED blink function in stacking. <pre>FS#led-blink enable FS#led-blink disable</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

7.8 session

	Use this command to perform redirection to a host or a device console.	
	session { device <i>switch_id</i> master }	
Parameter Description	Parameter	Description
	device	Redirects to the member device console.
	<i>switch_id</i>	Member device number, varying with products
	master	Redirects to the host console.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command takes effect in stacking mode.	
Configuration Examples	The following example redirects the serial port console of standby device 2 to the master device console. <pre>FS-STANDBY#session master</pre>	

	<pre>FS#exit FS-STANDBY#</pre> The following example redirects the master device console to the console of standby device 2 and exits. <pre>FS#session device 2 FS-STANDBY#exit FS#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.9 show switch id

	Use this command to display the device ID.	
	show switch id	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the device ID in the standalone mode. <pre>FS#show switch id Switch ID is 2</pre>	
	The following example displays the device ID in the stacking device. <pre>FS#show switch id Switch ID is 1</pre>	
Related Commands	Command	Description
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.10 show switch virtual

	Use this command to display the domain ID as well as the ID, status and role of the device.	
	show switch virtual	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the domain ID as well as the ID, status and role of the device in standalone mode. <pre>FS# show switch virtual Current system is running in "STANDALONE" mode.</pre> The following example displays the domain ID as well as the ID, status and role of each device in stacking mode. <pre>FS#show switch virtual Switch_id Domain_id Priority Status Role Description ----- 1(1) 1(1) 100(100) OK ACTIVE switch-1 2(2) 1(1) 100(100) OK CANDIDATE switch-2 3(3) 1(1) 100(100) OK STANDBY switch-3</pre>	
Related Commands	Command	Description
	switch	Modifies the device ID in standalone mode.
	switch priority	Configures the device priority.
	switch renumber	Modifies the device ID in vsu mode.
	switch domain	Modifies the domain ID of a device in vsu mode.
	switch virtual domain	Modifies the domain ID of a device in standalone mode.
Platform Description	N/A	

7.11 show switch virtual balance

	Use this command to display the load balance configuration in stacking mode.
	show switch virtual balance

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the load balance configuration of the device in stacking mode. FS#show switch virtual balance Aggregate port LFF: enable	
Related Commands	Command	Description
	show switch virtual	Displays the domain ID as well as the ID and role of the device.
Platform Description	N/A	

7.12 show switch virtual config

	Use this command to display the stacking configuration of the device in standalone or stacking mode.	
	show switch virtual config [<i>switch_id</i>]	
Parameter	Parameter	Description
Description	<i>switch_id</i>	Displays the stacking configuration of the specified device.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the stacking configuration of the device in standalone mode. <pre>FS#show switch virtual config mac: 00d0.f810.3323 ! switch virtual domain 1 ! switch 1 switch 1 priority 200 ! vsl-port port-member interface GigabitEthernet 0/1</pre>	

```
port-member interface GigabitEthernet 0/2
!
switch convert mode standalone
!
```

The following example displays the stacking configuration of the device in stacking mode.

```
FS#show switch virtual config
switch id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
switch 1 description switch1
!
vsl-port
port-member interface GigabitEthernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!

switch_id: 2 (mac: 00d0.f810.2222)
!
switch virtual domain 1
!
switch 2
switch 2 priority 100
!
vsl-port
port-member interface GigabitEthernet Ethernet 0/1
port-member interface GigabitEthernet 0/2
!
Switch convert mode virtual
!
```

The following example displays the stacking configuration of the device 1 in stacking mode.

```
FS#show switch virtual config 1
switch_id: 1 (mac: 00d0.f810.1111)
!
switch virtual domain 1
!
switch 1
switch 1 priority 200
```

	<pre>switch 1 description switch1 ! vsl-port port-member interface GigabitEthernet 0/1 port-member interface GigabitEthernet 0/2 !</pre>	
Related Commands	Command	Description
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.13 show switch virtual dual-active

	Use this command to display the configuration of DAD.	
	show switch virtual dual-active { bfd aggregateport summary }	
Parameter Description	Parameter	Description
	bfd	Configuration of BFD-based DAD
	aggregateport	Configuration of AP-based DAD
	summary	Configuration and status of DAD
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration and status of DAD. <pre>FS# show switch virtual dual-active summary BFD dual-active detection enabled: Yes Aggregateport dual-active detection enabled: No Interfaces excluded from shutdown in recovery mode: GigabitEthernet 1/0/3 GigabitEthernet 1/0/4 In dual-active recovery mode: No</pre>	
	The following example displays the configuration of BFD-based DAD. <pre>FS# show switch virtual dual-active bfd BFD dual-active detection enabled: Yes BFD dual-active interface configured: GigabitEthernet 1/0/1: UP GigabitEthernet 2/0/2: UP</pre>	

	The following example displays the status of AP-based DAD. <pre> FS# show switch virtual dual-active aggregateport Aggregateport dual-active detection enabled: Yes Aggregateport dual-active interface configured: AggregatePort 1: UP GigabitEthernet 1/0/1: UP GigabitEthernet 2/0/1: UP GigabitEthernet 1/0/2: UP GigabitEthernet 2/0/2: UP DAD relay enable AP list: AggregatePort 1 </pre>	
Related Commands	Command	Description
	dual-active detection	Enables DAD.
	dual-active pair interface	Configures a DAD interface.
	dual-active exclude interface	Configures an exclude interface.
Platform Description	N/A	

7.14 show switch virtual link

	Use this command to display the status of a virtual switch link (VSL).	
	show switch virtual link [port]	
Parameter Description	Parameter	Description
	port	Displays the port status of a VSL.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays VSL link information. <pre> FS# show switch virtual link VSL-AP State Peer-VSL Rx Tx Uptime ----- 1/1 UP 2/1 100000 100000 1d,4h,29m 2/1 UP 1/1 100000 100000 1d,4h,29m </pre>	
	The following example displays VSL port information. <pre> FS# show switch virtual link port </pre>	

	switch 1: <table><thead><tr><th>Port</th><th>AP</th><th>State</th><th>Peer-port</th><th>Rx</th><th>Tx</th><th>Uptime</th></tr></thead><tbody><tr><td>GigabitEthernet 1/0/1</td><td>1</td><td>OK</td><td>GigabitEthernet 2/0/1</td><td>9000</td><td>9000</td><td>0d,0h,20m</td></tr><tr><td>GigabitEthernet 1/0/2</td><td>2</td><td>OK</td><td>GigabitEthernet 2/0/2</td><td>9000</td><td>9000</td><td>0d,0h,20m</td></tr></tbody></table> Switch 2: <table><thead><tr><th>Port</th><th>AP</th><th>State</th><th>Peer-port</th><th>Rx</th><th>Tx</th><th>Uptime</th></tr></thead><tbody><tr><td>GigabitEthernet 2/0/1</td><td>1</td><td>OK</td><td>GigabitEthernet 1/0/1</td><td>9000</td><td>9000</td><td>0d,0h,20m</td></tr><tr><td>GigabitEthernet 2/0/2</td><td>2</td><td>OK</td><td>GigabitEthernet 1/0/2</td><td>9000</td><td>9000</td><td>0d,0h,20m</td></tr></tbody></table>								Port	AP	State	Peer-port	Rx	Tx	Uptime	GigabitEthernet 1/0/1	1	OK	GigabitEthernet 2/0/1	9000	9000	0d,0h,20m	GigabitEthernet 1/0/2	2	OK	GigabitEthernet 2/0/2	9000	9000	0d,0h,20m	Port	AP	State	Peer-port	Rx	Tx	Uptime	GigabitEthernet 2/0/1	1	OK	GigabitEthernet 1/0/1	9000	9000	0d,0h,20m	GigabitEthernet 2/0/2	2	OK	GigabitEthernet 1/0/2	9000	9000	0d,0h,20m
Port	AP	State	Peer-port	Rx	Tx	Uptime																																												
GigabitEthernet 1/0/1	1	OK	GigabitEthernet 2/0/1	9000	9000	0d,0h,20m																																												
GigabitEthernet 1/0/2	2	OK	GigabitEthernet 2/0/2	9000	9000	0d,0h,20m																																												
Port	AP	State	Peer-port	Rx	Tx	Uptime																																												
GigabitEthernet 2/0/1	1	OK	GigabitEthernet 1/0/1	9000	9000	0d,0h,20m																																												
GigabitEthernet 2/0/2	2	OK	GigabitEthernet 1/0/2	9000	9000	0d,0h,20m																																												
Related Commands	Command		Description																																															
	show switch virtual		Displays information about the vsusystem.																																															
	show switch virtual role		Displays the ID, role, and priority of each device.																																															
Platform Description	N/A																																																	

7.15 show switch virtual role

	Use this command to display the ID, role, and priority of each chassis.											
	show switch virtual role											
Parameter	Parameter		Description									
Description	N/A		N/A									
Defaults	N/A											
Command Mode	Privileged EXEC mode											
Usage Guide	N/A											
Configuration Examples	The following example displays the domain ID as well as the ID, status and role of the device in standalone mode. <pre>FS# show switch virtual Current system is running in "STANDALONE" mode.</pre> The following example displays the domain ID as well as the ID, status and role of each device in stacking mode. <pre>FS#show switch virtual</pre> <table><tr><td>Switch_id</td><td>Domain_id</td><td>Priority</td><td>Status</td><td>Role</td><td>Description</td></tr></table>						Switch_id	Domain_id	Priority	Status	Role	Description
Switch_id	Domain_id	Priority	Status	Role	Description							

	1(1)	1(1)	100(100)	OK	ACTIVE	switch-1
	2(2)	1(1)	100(100)	OK	CANDIDATE	switch-2
	3(3)	1(1)	100(100)	OK	STANDBY	switch-3
Related Commands	Command		Description			
	switch priority		Configures the priority of a device in the vsu system.			
	switch virtual domain		Modifies the domain ID of a device in standalone mode.			
	show switch virtual link		Displays VSL information.			
Platform Description	N/A					

7.16 show switch virtual topology

	Use this command to display the stacking topology connection status.	
	show switch virtual topology	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the topology status.	
	FS# show switch virtual topology	
	Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport num.	
	Chain Topology:	
	[1](1/2)---(2/1)[2]	
	Switch[1]: ACTIVE, MAC: 00d0.f822.33d6, Description: Switch1	
	Switch[2]: STANDBY, MAC: 1234.5678.9003, Description: Switch2	
	Field Description	
	Field	Description
	Ring Topology	Topology type.
	Switch[-]	Device description.
Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

7.17 switch

	Use this command to specify the ID of a device in the stacking system. Use the no form of this command to restore the default setting.	
	switch <i>switch_id</i>	
	no switch	
Parameter Description	Parameter	Description
	<i>switch_id</i>	ID of a device in the stacking system  The range depends on products.
Defaults	The default is 1.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	The device ID identifies each virtual device member. In stacking mode, the interface name format changes to "switch/slot/port" from "slot/port", in which "switch" is the device ID. If either chassis are active or if the role of the just started chassis is uncertain and both have the same priority, the chassis with a smaller ID is elected as the active one. This command can be only used to modify the device ID in standalone mode. In stacking mode, run the switch renumber command to modify the device ID. The modified device ID takes effect only after you restart the device, regardless of in standalone mode or in stacking mode.	
Configuration Examples	The following example sets the ID of the device whose domain ID is 1 to 2 in the stacking system. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 2 FS(config-vs-domain)# exit</pre>	
Related Commands	Command	Description
	switch virtual domain	Modifies the domain ID of a device in standalone mode.
	switch priority	Configures the priority of a device in the vsu system.
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.18 switch convert mode

	Use this command to perform conversion between the standalone mode and the stacking mode.
	switch convert mode { virtual standalone } [<i>switch_id</i>]

Parameter	Parameter	Description
Description	virtual	stacking mode
	standalone	Standalone mode
	<i>switch_id</i>	Device ID
Defaults	The device is in standalone mode by default.	
Command Mode	Privileged EXEC mode	
Usage Guide	After you run the switch convert mode virtual command, the software automatically backs up the configuration file in standalone mode, saves it as a standalone.text file, and then deletes the config.text file. The software also prompts you whether to use the virtual_switch.text file to overwrite the config.text file, write the stacking-related configurations to the config_vsu_dat file, and then restart the device. After you run the switch convert mode standalone command, the active chassis automatically backs up the configuration file in stacking mode, saves it as a virtual_switch.text file, and then deletes the config.text file. The active chassis also prompts you whether to use the standalone.text file to overwrite the config.text file and restart the device. The switch convert mode command can be used in standalone mode or in stacking mode. In standalone mode, this command is used to switch the mode of the current chassis. In stacking mode, this command is used to switch the mode of the device specified by switch_id if switch_id is available and to switch the mode of the active device if switch_id is not available. You are advised to first switch the mode of the standby device and then the mode of the active mode.	
Configuration Examples	The following example converts the device mode from the standalone mode into the stacking mode. <pre>FS# switch convert mode virtual</pre> The following example switches the modes of the standby device (switch_id set to 2) and the active device (switch_id set to 1) from the stacking mode to the standalone mode. <pre>FS# switch convert mode standalone 2 FS# switch convert mode standalone 1</pre>	
Related Commands	Command	Description
	switch	Modify the device ID in standalone mode.
	switch virtual domain	Modify the domain ID of a device in standalone mode.
	switch priority	Configure the priority of a device in the vsu system.
	show switch virtual	Display the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.19 switch crc

	Use this command to configure parameters for frame error detection. Use the no form of this command to restore the default setting.

	switch crc errors <i>error_num</i> times <i>time_num</i>	
	no switch crc	
Parameter	Parameter	Description
Description	<i>error_num</i>	Limits the number of error frames increasing from that in the last detection. If the increased number is greater than <i>error_num</i> , it is taken as an error.
	<i>time_num</i>	When the error count exceeds the <i>time_num</i> , the device will take actions (prompting a message or disabling the port).
Defaults	The default <i>error_num</i> is 3. The default <i>time_num</i> is 10.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the <i>error_time</i> and <i>time_num</i> parameters to 10 and 5 respectively. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# FS(config-vs-domain)#switch crc errors 10 times 5</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.20 switch description

	Use this command to configure the description for a stacking switch. Use the no form of this command to remove the setting.	
	switch <i>switch_id</i> description <i>dev-name</i>	
	no switch <i>switch_id</i> description	
Parameter	Parameter	Description
Description	<i>switch_id</i>	Device ID
	<i>dev_name</i>	Device description, no greater than 32 characters.
Defaults	N/A	
Command Mode	config-vs-domain configuration mode	
Usage Guide	This command is configured on a device in whether standalone or stacking mode and takes effect immediately after configuration,	

Configuration Examples	The following example configures the description for a stacking switch. FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 1 description buildingA FS(config-vs-domain)# exit	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.21 switch domain

	Use this command to modify the domain ID of a device in stacking mode. Use the no form of this command to restore the default setting.	
	switch <i>switch_id</i> domain <i>new_domain_id</i>	
	no switch <i>switch_id</i> domain	
Parameter	Parameter	Description
Description	<i>switch_id</i>	ID of the running device in stacking mode.  The range depends on products. For details, see the <i>Configuration Guide</i>.
	<i>new_domain_id</i>	New domain ID, in the range from 1 to 255.
Defaults	The default <i>new_domain_id</i> is 100 by default.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	Use this command only in stacking mode. In addition, the setting can take effect only after the device is restarted.	
Configuration Examples	The following example sets the domain ID of device 1 to 10 in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 1 domain 10</pre> The following example sets the domain ID of device 2 to 10 in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 2 domain 10</pre> The following example sets the domain ID of device 2 to the default value in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# no switch 2 domain</pre>	

Related Commands	Command	Description
	switch virtual domain	Modifies the domain ID in standalone mode.
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.22 switch priority

	Use this command to configure the priority of a device in the stacking system. Use the no form of this command to restore the default setting.	
	switch <i>switch_id</i> priority <i>priority_num</i>	
	no switch <i>switch_id</i> priority	
Parameter Description	Parameter	Description
	<i>switch_id</i>	ID of a device in the stacking system.  The range depends on products. For details, see the <i>Configuration Guide</i>.
	<i>priority_num</i>	Priority of a device in the stacking system, ranging from 1 to 255.
Defaults	The default <i>priority_num</i> is 100.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	A larger value means a higher priority. The chassis with a higher priority is elected as the active chassis. You can use this command in standalone mode or in stacking mode. The modified priority takes effect only after you restart the device. In stacking mode, switch_id indicates the ID of the running device. If the ID does not exist, the configuration does not effect.	
Configuration Examples	The following example sets the priority of device 1 to 200. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 1 priority 200 FS(config-vs-domain)# exit</pre> The following example sets the priority of device 1 to 200 and restores the priority of device 2 to the default value in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 1 priority 200 FS(config-vs-domain)# no switch 2 priority FS(config-vs-domain)# exit</pre>	

Related Commands	Command	Description
	switch	Modifies the device ID in standalone mode.
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.23 switch renumber

	Use this command to modify the ID of any device in stacking mode. Use the no form of this command to restore the default setting.	
	switch <i>switch_id</i> renumber <i>new_switch_id</i>	
	no switch <i>switch_id</i>	
Parameter Description	Parameter	Description
	<i>switch_id</i>	ID of the running device in stacking mode  The range depends on products. For details, see the <i>Configuration Guide</i> .
	<i>new_switch_id</i>	ID of the new switch  The range depends on products. For details, see the <i>Configuration Guide</i> .
Defaults	N/A	
Command Mode	config-vs-domain configuration mode	
Usage Guide	This command is configured in stacking mode. In addition and takes affect after device restart. The no form of this command will restore the switch ID to 1.	
Configuration Examples	The following example modifies the ID of device 1 that is running to 2 in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch 1 renumber 2</pre> The following example restores the ID of device 2 that is running to the default value in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# no switch 2</pre>	
Related Commands	Command	Description
	switch	Modifies the device ID in standalone mode.
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
Platform Description	N/A	

7.24 switch virtual aggregateport lff enable

	Use this command to enable the locally-preferred forwarding function on the AP in stacking mode. Use the no form of this command to disable this function.	
	switch virtual aggregateport lff enable	
	no switch virtual aggregateport lff enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the locally-preferred forwarding function on the AP in stacking mode. <pre>FS(config)# switch virtual domain 1 FS(config-vs-domain)# switch virtual aggregateport lff enable</pre>	
Related Commands	Command	Description
	show switch virtual balance	Displays the current traffic balancing mode.
Platform Description	N/A	

7.25 switch virtual domain

	Use this command to modify the domain ID of a device in standalone mode, or enter config-vs-domain configuration mode in stacking mode.	
	Use the no form of this command to restore the default setting.	
	switch virtual domain domain_id	
	no switch virtual domain	
Parameter	Parameter	Description
Description	<i>domain_id</i>	Domain ID of the stacking, in the range from 1 to 255.
Defaults	The default is 100.	
Command Mode	Global configuration mode	
Usage Guide	Only two devices with the same domain ID can form a virtual device. The domain ID must be unique within the local area network (LAN).	

Configuration	The following example sets the domain ID of the stacking to 1 in standalone mode.	
Examples	FS(config)# switch virtual domain 1 FS(config-vs-domain)#	
Related Commands	Command	Description
	show switch virtual	Displays the domain ID as well as the ID and role of each chassis.
	switch domain	Modifies the domain ID in vsu mode.
Platform Description	N/A	

7.26 switch virtual ecmp lff enable

	Use this command to enable the locally-preferred forwarding function on the ECMP interface in stacking mode. Use the no form of this command to disable this function.	
	switch virtual ecmp lff enable	
	no switch virtual ecmp lff enable	
Parameter		
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	config-vs-domain configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the locally-preferred forwarding function on the ECMP interface in stacking mode. FS(config)# switch virtual domain 1 FS(config-vs-domain)#switch virtual ecmp lff enable	
Related Commands	Command	Description
	show switch virtual balance	Displays the current load balance mode.
Platform Description	N/A	

7.27 vsl-port

	Use this command to enter VSL-PORT mode
	vsl-port

Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is configured on a device in whether standalone mode or stacking mode.	
Configuration Examples	The following example enters VSL-AP configuration mode on a device in standalone mode. <pre>FS(config)# vsl-port FS(config-vsl-port)#</pre> The following example enters VSL-APPORT configuration mode on a device in stacking mode. <pre>FS(config)# vsl-port FS(config-vsl-port)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8 RNS &Track Commands

8.1 delay

	Use this command to specify a period of time after which the tracked object status will change if the interface status changes. Use the no form of this command to restore the default setting.	
	delay { up <i>seconds</i> [down <i>seconds</i>] [up <i>seconds</i>] down <i>seconds</i> }	
	no delay	
Parameter Description	Parameter	Description
	up <i>seconds</i>	Sets the delay time from down to up in the range from 0 to 180. The unit is second.
	down <i>seconds</i>	Sets the delay time from up to down in the range from 0 to 180. The unit is second.
Defaults	There is no delay by default.	
Command Mode	Track configuration mode	
Usage Guide	The continual oscillation of the tracked object status may cause the client of this tracked object changing also. This command can be used to delay advertising the change of the tracked object status. For example, the status of a tracked object changes from up to down, if the delay down 180 is configured, the down status will be advertised after 180 seconds. If the tracked object status changes to the up again in this period, it won't be advertised. For the client of the tracked object, the status of the tracked object is always up.	
Configuration Examples	The following example sets the delay time to 30 seconds when the tracked object changes to up from down. <pre>FS(config)# track 5 rns 10 FS(config-track)# delay up 30 FS(config-track)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.2 dns

	Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode.	
	dns { <i>destination-hostname</i> name-server <i>a.b.c.d</i> [source-ipaddr <i>ip-address</i>] [out-interface <i>type num</i> [next-hop <i>A.B.C.D</i>]] } oob <i>destination-hostname</i> name-server <i>a.b.c.d</i> [source-ipaddr <i>ip-address</i>] via <i>type num</i> next-hop <i>A.B.C.D</i> }	
Parameter Description	Parameter	Description
	<i>destination-hostname</i>	Sets the destination IP address or the destination host domain name.
	oob	Enables management port detection.
	<i>a.b.c.d</i>	Sets the IP address for the DNS server.
	<i>ip-address</i>	Indicates the source IP address of RNS packets.
	out-interface <i>type num</i>	Specifies the egress interface (non-management port) for RNS packets.
	via <i>type num</i>	Specifies the management port as the egress interface (non-management port) for RNS packets.
	<i>A.B.C.D</i>	Specifies the next-hop IP address for RNS packets.
Defaults	N/A	
Command Mode	IP RNS configuration mode	
Usage Guide	Use this command to set an IP RNS object to send the DNS packets and to enter the IP RNS DNS mode. If you want to change the probe type, you should delete the probe first by using the no ip rns command and then perform new configuration.	
Configuration Examples	The following example sets the IP RMS object to send the DNS packets. <pre> FS(config)# ip rns 1 FS(config-ip-rns)# dns www.FS.com.cn name-server 61.154.22.41 FS(config-ip-rns-dns)# exit FS(config)# ip rns schedule 1 start-time now </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.3 frequency

	Use this command to set the interval of sending the packets, which must be no smaller than the timeout time. Use the no form of this command to restore the default setting.	
	frequency <i>milliseconds</i>	
	no frequency	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	Sets the interval of sending the packets, in the range from 10 to 604,800,000 in the unit of milliseconds.
Defaults	The default is 60 seconds.	
Command Mode	IP RNS ICMP echo configuration mode IP RNS DNS configuration mode IP RNS TCP configuration mode	
Usage Guide	Use this command to set the interval of sending the ICMP echo or DNS packets, which must accord with the following formula to ensure accuracy: frequency <i>milliseconds</i> > timeout <i>milliseconds</i> >= threshold <i>milliseconds</i>	
Configuration Examples	The following example configures an ICMP echo probe whose destination address is 192.168.21.1. The frequency, timeout time and threshold are set to 30,000, 8,000 and 6,000 milliseconds respectively. <pre> FS(config-ip-rns)#icmp-echo 192.168.21.1 FS(config-ip-rns-icmp-echo)#frequency 30000 FS(config-ip-rns-icmp-echo)#timeout 8000 FS(config-ip-rns-icmp-echo)#threshold 6000 </pre>	
Related Commands	Command	Description
	timeout	Defines the timeout time of sending the packets.
Platform Description	N/A	

8.4 icmp-echo

	Use this command to configure an ICMP echo RNS probe.
	icmp-echo { <i>destination-ip-address</i> <i>destination-hostname</i> [name-server <i>ip-address</i>] } [source-ipaddr <i>ip-address</i>] [out-interface <i>type num</i> [next-hop <i>A.B.C.D</i>]] oob { <i>destination-ip-address</i> <i>destination-hostname</i> [name-server <i>ip-address</i>] } [source-ipaddr <i>ip-address</i>] via <i>type num next-hop A.B.C.D</i>

Parameter Description	Parameter	Description
	<i>destination-hostname</i>	Sets the destination IP address for the ICMP echo packets.
	oob	Enables management port detection.
	<i>destination-hostname</i>	Sets the destination host name within 127 characters. The exceeding characters are truncated automatically.
	name-server <i>ip-address</i>	Sets the domain name server. The default domain name server is configured via the ip name-server command.
	source-ipaddr <i>ip-address</i>	Sets the source IP address for the ICMP echo packets.
	out-interface <i>type num</i>	Sets the egress port(non-management) for the probe packet.
	via <i>type num</i>	Specifies the management port as the egress interface (non-management port) for probe packets.
	next-hop <i>A.B.C.D</i>	Sets the next hop IP address.
Defaults	N/A	
Command Mode	IP RNS configuration mode	
Usage Guide	This command is used to enable the IP RNS object to send ICMP echo packets containing the specified destination IP address. The default payload size of an ICMP echo packet is 36 bytes. The request-data-size command is used to modify the packet size. You can modify the probe parameter after specifying the type of the IP RNS probe (such as ICMP echo probe). If you want to change the probe type, you should delete the probe first by using the no ip rns command and then perform new configuration.	
Configuration Examples	The following example enables the IP RNS object to send the ICMP echo packets containing the destination IP address 10.1.1.1. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# exit FS(config)# ip rns schedule 1 start-time now life forever</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.5 ip rns

Use this command to define an IP RNS operation object and to enter the IP RNS configuration mode.

Use the **no** form of this command to delete an IP RNS operation object.

	ip rns <i>operation-number</i> [{ dns <i>destination-hostname</i> name-server <i>ip-address</i> icmp-echo <i>destination-ip-address</i> tcp-connect <i>destination-ip-address</i> <i>port-number</i> } [frequency <i>seconds</i>] [timeout <i>milliseconds</i>] [threshold <i>milliseconds</i>]]]	
	no ip rns <i>operation-number</i>	
Parameter Description	Parameter	Description
	<i>operation-number</i>	Sets the IP RNS operation object number, in the range from 1 to 500.
	dns <i>destination-hostname</i> name-server <i>ip-address</i>	Brief DNS detection configuration. <i>destination-hostname</i> : Indicates the destination host name. A maximum of 127 characters can be entered. Characters out of this limit will be truncated. name-server <i>ip-address</i> : Indicates the IP address of the DNS server.
	icmp-echo <i>destination-ip-address</i>	Brief ICMP-echo detection configuration. <i>destination-ip-address</i> : Indicates the destination IP address.
	tcp-connect <i>destination-ip-address</i> <i>port-number</i>	Brief TCP-connect detection configuration. <i>destination-ip-address</i> : Indicates the destination IP address. <i>port-number</i> : Indicates the TCP port to be detected.
	frequency <i>seconds</i>	Sets the detection interval. For details, see the frequency command.
	timeout <i>milliseconds</i>	Sets the timeout time for one IP RNS detection operation. For details, see the timeout command.
	threshold <i>milliseconds</i>	Sets the upper threshold for one IP RNS detection operation. For details, see the threshold command.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Currently, the RNS supports only IPv4-related tests, but not IPv6-related tests. At most 500 tests can be configured, depending on the performance of devices. The test function is only a value-added function. When a large number of tests are configured and consume a lot of system resources, the test function may be temporary disabled to ensure normal operation of core services, such as route forwarding. Detailed configuration (executing mandatory items of ip rns operation-number): Run this command and enter the IP-RNS configuration mode. In this mode, you can define various test types. If the test type is not configured, the RNS test is not created. After configuring an RNS test, you must run the ip rns schedule command to configure its schedule parameters; otherwise, the test cannot be conducted. After configuring the type of an RNS test, you can run the ip rns command to enter the mode of the test type. To modify the type of an RNS instance, you need to first delete the RNS instance by running the no ip rns command in global configuration mode.	
Configuration Examples	The following example defines the IP RNS object 1. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# threshold 10000</pre>	

	<pre>FS(config-ip-rns-icmp-echo)# timeout 20000 FS(config-ip-rns-icmp-echo)# frequency 30000 FS(config-ip-rns-icmp-echo)# exit FS(config)# ip rns schedule 1 start-time now life forever</pre>	
Related Commands	Command	Description
	show ip rns statistics	Displays the statistical data on the IP RNS object.
Platform Description	N/A	

8.6 ip rns reaction-configuration

	Use this command to configure proactive threshold monitoring and trigger for the IP RNS probe. Use the no form of this command to restore the default setting.	
	<pre>ip rns reaction-configuration operation-number react monitored-element [action-type option] [threshold-type { average [number-of-measurements] consecutive [occurrences] immediate never xofy [x-value y-value] }] [threshold-value upper-threshold lower-threshold]</pre>	
	<pre>no ip rns reaction-configuration operation-number [react monitored-element]</pre>	
Parameter Description	Parameter	Description
	<i>operation-number</i>	Operation index, in the range from 1 to 500.
	<i>monitored-element</i>	- Monitored element. The available parameters are listed as follows: allfail: Failed to monitor all elements. The default action-type is track. This parameter is applied on the track module for communication. rtt: Packet round trip time (RTT) exceeds the threshold range. timeout: Timeout in whatever direction.
	action-type <i>option</i>	- The available parameters include: none: No action, which is the default setting trigger: Only supports the trigger action. track: Only supports the track action. Only when monitored-element is allfail is this parameter supported, which is available exclusively.
	average [<i>number-of-measurements</i>]	Triggers operation when the average value of number-of-measurements consecutive times exceeds the threshold range. For example, <i>number-of-measurements</i> is set to three. Upper and lower thresholds are 5000 and 4000 respectively. The average value for three consecutive measurements 6000, 6000, 5000 is (6000+6000+5000)/3=5667, exceeding the upper threshold 5000. The valid range is from 1 to 16 and the default is 5.
	consecutive [<i>occurrences</i>]	Triggers operation when the value of monitored element exceeds the

		threshold range for <i>occurrences</i> consecutive times. The valid range is from 1 to 16. The default is 5.																						
	immediate	Triggers operation immediately when the value of monitored element exceeds the threshold range.																						
	never	Never triggers operation.																						
	xofy [x-value y-value]	X probes among the latest Y ones exceed the threshold range. The valid X range is from 1 to 16 and the default is 5. The valid Y range is from 1 to 16 and the default is 5.																						
	threshold-value <i>upper-threshold lower-threshold</i>	Configures upper and lower thresholds. When <i>monitored-element</i> is rtt , this parameter indicates time, in the range from 0 to 60,000 milliseconds. See Usage Guide for the default setting. When react type is timeout, you don't need to configure this parameter.																						
Defaults	N/A																							
Command Mode	Global configuration mode																							
Usage Guide	One IP RNS object can be configured with multiple thresholds monitoring, each for one element. Monitored elements that are supported vary with different probe types. <table><tr><th>monitored-element</th><th>icmp-echo</th><th>dns</th><th>tcp-connect</th></tr><tr><td>timeout</td><td>ü</td><td>ü</td><td>ü</td></tr><tr><td>rtt</td><td>ü</td><td>ü</td><td>ü</td></tr></table> The default thresholds for monitored elements are listed as follows: <table><tr><th>Monitored Element</th><th>Upper Threshold</th><th>Lower Threshold</th></tr><tr><td>timeout</td><td>-</td><td>-</td></tr><tr><td>rtt</td><td>5000 ms</td><td>0 ms</td></tr></table>			monitored-element	icmp-echo	dns	tcp-connect	timeout	ü	ü	ü	rtt	ü	ü	ü	Monitored Element	Upper Threshold	Lower Threshold	timeout	-	-	rtt	5000 ms	0 ms
monitored-element	icmp-echo	dns	tcp-connect																					
timeout	ü	ü	ü																					
rtt	ü	ü	ü																					
Monitored Element	Upper Threshold	Lower Threshold																						
timeout	-	-																						
rtt	5000 ms	0 ms																						
Configuration Examples	The following example configures RNS1 and its threshold monitoring. FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 192.168.23.1 FS(config-ip-rns-icmp-echo)# exit FS(config)# ip rns schedule 1 start-time now life forever FS(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type triggerOnly																							
Related Commands	Command	Description																						
	N/A	N/A																						
Platform Description	N/A																							

8.7 ip rns reaction-trigger

	Use this command to enable the IP RNS probe which exceeds the monitoring threshold to trigger another IP RNS probe which is in the pending state. Use the no form of this command to restore the default setting.	
	ip rns reaction-trigger <i>operation-number target-operation</i>	
	no ip rns reaction-trigger <i>operation-number target-operation</i>	
Parameter Description	Parameter	Description
	<i>operation-number</i>	The source operation number, in the range from 1 to 500
	<i>target-operation</i>	The target operation number, in the range from 1 to 500
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	The trigger function is applied in network fault diagnosis scenario	
Configuration Examples	The following example enables IP RNS1 to trigger IP RNS 2. <pre> FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo www.google.com FS(config-ip-rns-icmp-echo)# exit FS(config)#ip rns schedule 1 start-time now life forever FS(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger FS(config)# ip rns 2 FS(config-ip-rns)# dns www.baidu.com name-server 8.8.8.8 FS(config-ip-rns-dns)# exit FS(config)#ip rns reaction-trigger 1 2 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.8 ip rns reset

	Use this command to clear all IP RNS configuration.
	ip rns reset

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to clear all IP RNS configuration. This command is used only in extreme cases (for example, RNS probe configuration is wrong).	
Configuration Examples	The following example clears all IP RNS configuration. FS(config)# ip rns reset	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.9 ip rns restart

	Use this command to restart the IP RNS probe.	
	ip rns restart <i>operation-number</i>	
Parameter Description	Parameter	Description
	<i>operation-number</i>	Sets the IP RNS operation object number, in the range from 1 to 500.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to restart the IP RNS probe whose schedule is in the pending state. This command is invalid for the IP RNS probe not configured with the scheduling policy.	
Configuration Examples	The following example restarts IP RNS 1. FS(config)# ip rns restart 1	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.10 ip rns schedule

	Use this command to configure the scheduling strategy, start time and survival time for the IP RNS probe. Use the no form of this command to restore the default setting.	
	ip rns schedule operation-number [life { forever seconds }] [start-time { hh:mm [:ss] [month day day month] pending now after hh:mm:ss }] [recurring]	
	no ip rns schedule operation-number	
Parameter Description	Parameter	Description
	operation-number	RNS operation index, in the range from 1 to 500
	life forever	The RNS operation is valid forever.
	life seconds	The RNS survival time, measured in seconds
	hh:mm [:ss]	Defines the time when the operation starts,
	month	The month when the operation starts, in the range from January (Jan.) to December (Dec.). The default is the current month.
	day	The day when the operation starts, in the range from 1 to 31. The default is the current day.
	pending	The start time is pending.
	now	The operation starts right now.
	after hh:mm:ss	The operation starts after hh hours, mm minutes and ss seconds.
	recurring	The operation starts automatically as scheduled every day.
Defaults	The IP RNS probe is in the pending state by default. In other words, the probe is not performed unless it is triggered by another RNS probe.	
Command Mode	Global configuration mode	
Usage Guide	The ip rns schedule command is used to configure the IP RNS probe with scheduling policy. Once the scheduling policy is configured, the RNS probe cannot be modified. You can modify the RNS probe after deleting the schedule with the no ip rns schedule command. Life {seconds} refers to the survival time of the IP RNS probe. The probe will end after the survival time.	
Configuration Examples	The following example configures the RNS probe with scheduling policy. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1</pre>	

	<pre>FS(config-ip-rns-icmp-echo)# exit FS(config)#ip rns schedule 1 start-time now life forever</pre> Once the scheduling policy is configured, the RNS probe cannot be modified. The RNS probe can be modified after the schedule is deleted. <pre>FS(config)# ip rns 1</pre> Entry already running and cannot be modified (only can delete (no) and start over) (check to see if the probe has finished exiting) <pre>FS(config)# no ip rns schedule 1 FS(config)# ip rns 1 FS(config-ip-rns-icmp-echo)# exit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.11 object

	Use this command to add a tracked object to the object track list. Use the no form of this command to delete a traced object.	
	object <i>object-number</i> [not]	
	no object <i>object-number</i>	
Parameter Description	Parameter	Description
	<i>object-number</i>	Tracked object number, in the range from 1 to 700
Defaults	No tracked object is configured by default.	
Command Mode	Track configuration mode	
Usage Guide	This command is used to add a tracked object to the object track list. The number of tracked objects is only restricted by the track list capacity. object <i>object-number</i>: The tracked object must be in the up state for the track list to be in the up state. object <i>object-number</i> not: track: The tracked object must be in the up state for the track list to be in the up state, ● This command is configured only in track configuration mode for the track list. ● The object cannot track itself. ● The objects cannot track each other. For example, if A tracks B, B cannot track A. Otherwise, both A and B are in oscillation.	

Configuration Examples	The following example adds tracked object 4 to the object track list. When object 1 is in the up state, 2 down, 3 up, object 4 is in the up state. <pre>FS(config)# track 4 list boolean and FS(config-track)# object 1 FS(config-track)# object 2 not FS(config-track)# object 3 FS(config-track)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.12 request-data-size

	Use the following example to set the protocol payload size of IP RNS probe packet. Use the no form of this command to restore the default setting.		
	request-data-size <i>bytes</i>		
	no request-data-size		
Parameter Description	Parameter	Description	
	<i>bytes</i>	The number of payload bytes. The minimum/maximum number of bytes varies with the probe type.	
Defaults	The default is the minimum payload byte, which varies with the probe type.		
Command Mode	IP RNS ICMP echo configuration mode		
Usage Guide	This command is used to fill bytes in the probe packet to probe for the bigger packet.		
	Probe Type	Range	Default
	icmp-echo	[36, 1472]	36
Configuration Examples	The following example sets the protocol payload size of the IP RNS probe packet to 50.		
	<pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# request-data-size 50 FS(config-ip-rns-icmp-echo)# exit</pre>		

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.13 show ip rns collection-statistics

	Use this command to display statistics about the RNS probe.									
	show ip rns collection-statistics [<i>operation-number</i>]									
Parameter Description	Parameter	Description								
	<i>operation-number</i>	Sets the IP RNS operation object number, in the range from 1 to 500. The default is all IP RNS operation objects.								
Defaults	N/A									
Command Mode	Privileged EXEC mode									
Usage Guide	This command is used to display statistics about an IP RNS probe.									
Configuration Examples	The following example displays statistics about the all RNS probes. <pre>FS#show ip rns collection-statistics 1 Entry number: 1 Start Time Index: *2014-03-20 19:53:51 Number of successful operations: 919 Number of operations over threshold: 0 Number of failed operations due to a Disconnect: 0 Number of failed operations due to a Timeout: 2 Number of failed operations due to a Busy: 0 Number of failed operations due to a No Connection: 0 Number of failed operations due to an Internal Error: 2 Number of failed operations due to a Sequence Error: 0 Number of failed operations due to a Verify Error: 0 RTT Values: RTTAvg: 18 RTTMin: 16 RTTMax: 37 NumOfRTT: 919 RTTSum: 16654 RTTSum2: 302786</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Entry number</td><td>IP RNS operation index</td></tr><tr><td>Start Time Index:</td><td>Schedule start time</td></tr><tr><td>Number of successful operations:</td><td>Number of successful operation.</td></tr></table>		Field	Description	Entry number	IP RNS operation index	Start Time Index:	Schedule start time	Number of successful operations:	Number of successful operation.
Field	Description									
Entry number	IP RNS operation index									
Start Time Index:	Schedule start time									
Number of successful operations:	Number of successful operation.									

	Number of operations over threshold:	Number of threshold violation
	Number of failed operations due to a Disconnect:	Number of operation failure due to disconnection
	Number of failed operations due to a Timeout:	Number of operation failure due to timeout
	Number of failed operations due to a Busy:	Number of operation failure since the peer end is busy
	Number of failed operations due to a No Connection:	Number of operation failure due to no connection
	Number of failed operations due to an Internal Error:	Number of operation failure due to internal error
	Number of failed operations due to a Sequence Error:	Number of operation failure due to sequence error
	Number of failed operations due to a Verify Error:	Number of operation failure due to verification error
	RTT Values	RTT value
	RTTAvg:	Average RTT value
	RTTMin:	Minimum RTT value
	RTTMax:	Maximum RTT value
	NumOfRTT:	Number of counting RTT value
	RTTSum:	Sum of RTT value
	RTTSum2:	Sum of squares of RTT value
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.14 show ip rns configuration

	Use this command to display the RNS instance configuration.	
	show ip rns configuration [<i>operation-number</i>]	
Parameter Description	Parameter	Description
	<i>operation-number</i>	Sets the RNS instance number, in the range from 1 to 500.
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the RNS instance configuration. The configuration varies with different packet types.	
Configuration Examples	The following example displays the RNS 1 configuration. FS# show ip rns configuration 1	

	Entry number: 1 Tag: FS555 Type of operation to perform: icmp-echo Operation timeout (milliseconds): 5000 Operation frequency (milliseconds): 10000 Threshold (milliseconds): 5000 Recurring (Starting Everyday): FALSE Life (seconds): 3500 Next Scheduled Start Time:Start Time already passed Target address/Source address: 2.2.2.3/0.0.0.0 Request size (ARR data portion): 36	
	Field	Description
	Entry number	IP RNS operation index
	Tag	Instance tag.
	Type of operation to perform	Operation type.
	Operation timeout (milliseconds)	Operation timeout.
	Operation frequency (milliseconds)	Operation frequency.
	Threshold (milliseconds)	Threshold.
	Recurring (Starting Everyday)	The operation starts every day.
	Life (seconds)	Life time
	Next Scheduled Start Time	Next scheduled start time.
	Target address/Source address	Target address/Source address
	Request size (ARR data portion)	Request packet size.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.15 show ip rns operational-state

Use this command to display operational state.		
show ip rns operational-state [<i>operation-number</i>]		
Parameter Description	Parameter	Description
	<i>operation-number</i>	Sets the IP RNS operation object number, in the range from 1 to 500. The default is all RNS operation objects.
Defaults	N/A	
Command	Privileged EXEC mode	

Mode																														
Usage Guide	This command is used to display the state information about an RNS probe.																													
Configuration Examples	The following example displays the state information about all RNS probes. <pre>FS# show ip rns operational-state Entry number: 1 Modification time: *2014-01-10 10:26:14 Current seconds left in Life: Forever Operational state of entry: Active Number of Octets Used by this Entry: 2272 Number of operations attempted: 232 Number of operations skipped: 0 Connection loss occurred: FALSE Timeout occurred: FALSE Over thresholds occurred: FALSE Latest RTT (milliseconds): 4 Latest operation start time: 2014-01-10 10:26:55 Latest operation return code: OK</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Entry number</td><td>IP RNS operation index</td></tr><tr><td>Modification time</td><td>Probe result recounting time (every time schedule is enabled, the result is counted again).</td></tr><tr><td>Number of Octets Used by this Entry</td><td>Number of octets contained in the probe packet.</td></tr><tr><td>Number of operations attempted</td><td>Number of attempted operation.</td></tr><tr><td>Number of operations skipped</td><td>Number of failed operation.</td></tr><tr><td>Current seconds left in Life</td><td>Probes for the left life.</td></tr><tr><td>Operational state of entry</td><td>Probes for the operational state (Active/Disactive).</td></tr><tr><td>Connection loss occurred</td><td>Connection loss occurred.</td></tr><tr><td>Timeout occurred</td><td>Send request timeout occurred,</td></tr><tr><td>Over thresholds occurred</td><td>Threshold violation occurred.</td></tr><tr><td>Latest RTT (milliseconds)</td><td>Latest RTT.</td></tr><tr><td>Latest operation start time</td><td>Latest operation start time.</td></tr><tr><td>Latest operation return code</td><td>Latest operation return code.</td></tr></table>		Field	Description	Entry number	IP RNS operation index	Modification time	Probe result recounting time (every time schedule is enabled, the result is counted again).	Number of Octets Used by this Entry	Number of octets contained in the probe packet.	Number of operations attempted	Number of attempted operation.	Number of operations skipped	Number of failed operation.	Current seconds left in Life	Probes for the left life.	Operational state of entry	Probes for the operational state (Active/Disactive).	Connection loss occurred	Connection loss occurred.	Timeout occurred	Send request timeout occurred,	Over thresholds occurred	Threshold violation occurred.	Latest RTT (milliseconds)	Latest RTT.	Latest operation start time	Latest operation start time.	Latest operation return code	Latest operation return code.
Field	Description																													
Entry number	IP RNS operation index																													
Modification time	Probe result recounting time (every time schedule is enabled, the result is counted again).																													
Number of Octets Used by this Entry	Number of octets contained in the probe packet.																													
Number of operations attempted	Number of attempted operation.																													
Number of operations skipped	Number of failed operation.																													
Current seconds left in Life	Probes for the left life.																													
Operational state of entry	Probes for the operational state (Active/Disactive).																													
Connection loss occurred	Connection loss occurred.																													
Timeout occurred	Send request timeout occurred,																													
Over thresholds occurred	Threshold violation occurred.																													
Latest RTT (milliseconds)	Latest RTT.																													
Latest operation start time	Latest operation start time.																													
Latest operation return code	Latest operation return code.																													
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A																									
Command	Description																													
N/A	N/A																													
Platform Description	N/A																													

8.16 show ip rns reaction-configuration

	Use this command to display the proactive threshold monitoring information of an IP RNS probe.									
	show ip rns reaction-trigger [operation-number]									
Parameter Description	Parameter	Description								
	operation-number	The number of IP RNS operation objects, in the range from 1 to 500. The default is all RNS operation objects.								
Defaults	N/A									
Command Mode	Privileged EXEC mode									
Usage Guide	This command is used to display the proactive threshold monitoring information of an IP RNS probe.									
Configuration Examples	The following example displays the proactive threshold monitoring information of all IP RNS probes. FS#show ip rns reaction-configuration Entry number: 1 Reaction: rtt Threshold Type: Never Rising (milliseconds): 5000 Falling (milliseconds): 3000 Threshold Count: 5 Threshold Count2: 5 Action Type: trigger Reaction: timeout Threshold Type: Never Threshold Count: 5 Threshold Count2: 5 Action Type: trigger <table><tr><th>Field</th><th>Description</th></tr><tr><td>Entry number</td><td>IP RNS operation index</td></tr><tr><td>Reaction</td><td>Monitored object</td></tr><tr><td>Threshold Type</td><td> The available parameters are listed as follows: never: Never triggers operation. consecutive: Triggers operation when the value of monitored element exceeds the threshold range for occurrences consecutive times. average: Triggers operation when the average value of number-of-measurements consecutive times exceeds the threshold range. immediate: Triggers operation immediately when the </td></tr></table>		Field	Description	Entry number	IP RNS operation index	Reaction	Monitored object	Threshold Type	The available parameters are listed as follows: never: Never triggers operation. consecutive: Triggers operation when the value of monitored element exceeds the threshold range for occurrences consecutive times. average: Triggers operation when the average value of number-of-measurements consecutive times exceeds the threshold range. immediate: Triggers operation immediately when the
Field	Description									
Entry number	IP RNS operation index									
Reaction	Monitored object									
Threshold Type	The available parameters are listed as follows: never: Never triggers operation. consecutive: Triggers operation when the value of monitored element exceeds the threshold range for occurrences consecutive times. average: Triggers operation when the average value of number-of-measurements consecutive times exceeds the threshold range. immediate: Triggers operation immediately when the									

		value of monitored element exceeds the threshold range. xofy : X probes among the latest Y ones exceed the threshold range.
	Rising (milliseconds)	Upper threshold
	Falling (milliseconds)	Lower threshold
	Threshold Count	The parameter refers to the x value when the threshold-type is xofy or the average count when the threshold-type is average .
	Threshold Count2	The parameter refers to the y value when the threshold-type is xofy or the consecutive count when the threshold-type is consecutive .
	Action Type	Action type
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.17 show ip rns reaction-trigger

	Use this command to display the reaction trigger information for all RNS objects.	
	show ip rns reaction-trigger [<i>operation-number</i>]	
Parameter Description	Parameter	Description
	<i>operation-number</i>	The number of IP RNS operation object, in the range from 1 to 500. The default is all RNS operation objects.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the reaction trigger information for all RNS objects.	
Configuration Examples	The following example displays the reaction trigger information for all RNS objects. <pre>FS#show ip rns reaction-trigger Entry number: 1 Target rns index: 2 Status of Entry (SNMP RowStatus): active Operational State: pending</pre>	

	Field	Description
	Entry number	RNS index
	Target rns index	Target RNS index
	Status of Entry (SNMP RowStatus)	Status of RNS entry
	Operational State	Reaction-trigger state
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.18 show ip rns statistics

	Use this command to display the RNS object statistics.	
	show ip rns statistics [<i>operation-number</i>]	
Parameter Description	Parameter	Description
	<i>operation-number</i>	Sets the IP RNS operation object number, in the range from 1 to 500
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	The statistics vary with different packet types.	
Configuration Examples	The following example displays the RNS object statistics. FS#show ip rns statistics 1 Round trip time(RTT) Index 1 Operation time to live: Forever Latest RTT: 1 ms Latest operation start time: 2014-01-20 10:21:38 Latest operation return code: OK Number of successes: 386 Number of failures: 12	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

8.19 show track

	Use this command to display statistics of the tracked object.													
	show track [<i>track-number</i>]													
Parameter Description	Parameter	Description												
	<i>track-number</i>	Sets the tracked object number, in the range from 1 to 700.												
Defaults	N/A													
Command Mode	Privileged EXEC mode													
Usage Guide	N/A													
Configuration Examples	The following example displays statistics of all tracked objects. <pre>FS#show track Track 1 Reliable Network Service 5 The state is Up 1 change, current state last: 120 secs Delay up 30 secs, down 50 secs Track 3 Interface FastEthernet 1/0 The state is Down, delayed Up (5 secs remaining) 3 change, current state last: 300 secs Delay up 60 secs, down 60 secs Track 4 List boolean and Object 1 Object 2 not The state is Up 1 change, current state last: 100 secs Delay up 0 secs, down 0 secs</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Track x</td><td>Tracked object ID</td></tr><tr><td>Reliable Network Service x</td><td>Tracked RNS object</td></tr><tr><td>The state is x</td><td>Tracked object state</td></tr><tr><td>x change</td><td>Tracked object change count</td></tr><tr><td>current state last: x secs</td><td>The time for which the current state lasts</td></tr></table>		Field	Description	Track x	Tracked object ID	Reliable Network Service x	Tracked RNS object	The state is x	Tracked object state	x change	Tracked object change count	current state last: x secs	The time for which the current state lasts
Field	Description													
Track x	Tracked object ID													
Reliable Network Service x	Tracked RNS object													
The state is x	Tracked object state													
x change	Tracked object change count													
current state last: x secs	The time for which the current state lasts													

	Delay up x secs, down x secs	The delay state of the tracked object
	Interface x x	Tracked interface
	The state is x, delayed y (c secs remaining)	The tracked object state is x, and will turn to y in c seconds.
	List boolean and	The Boolean expression enables calculation by using “and” operator.
	Object x	Object x is in the up state.
	Object x not	Object x is in the down state.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.20 tag

	Use this command to set the tag for IP RNS probe. Use the no form of this command to restore the default setting.	
	tag <i>text</i>	
	no tag	
Parameter Description	Parameter	Description
	<i>text</i>	Sets the tag for IP RNS probe, which is composed of up to 79 printable characters.
Defaults	N/A	
Command Mode	IP RNS DNS configuration mode IP RNS ICMP echo configuration mode	
Usage Guide	Tag is used to identify the probe. When the tag exceeds 79 characters, the surplus characters are truncated.	
Configuration Examples	The following example sets the tag for IP RNS probe to telecom gateway. FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# tag telecom_gateway FS(config-ip-rns-icmp-echo)# exit	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

8.21 tcp-connect

	Use this command to configure TCP connectivity probe.	
	tcp-connect { <i>destination-ip-address</i> <i>destination-hostname</i> [name-server <i>ip-address</i>] } <i>port-number</i>	
Parameter Description	Parameter	Description
	<i>destination-ip-address</i>	Destination IP address
	<i>destination-hostname</i>	Destination domain name
	name-server <i>ip-address</i>	IP address of the DNS server
	<i>port-number</i>	TCP port number
Defaults	N/A	
Command Mode	IP RNS configuration mode	
Usage Guide	TCP connectivity probe detects the connection with the TCP server. If no peer TCP server exist, enable the IP RNS server function on peer FS devices.	
Configuration Examples	The following example configures TCP connectivity probe. <pre>FS(config)# ip rns 1 FS(config)# tcp-connect www.FS.net name-server 8.8.8.8 999 FS(config-ip-rns-tcp-connect)# exit FS(config)# ip rns schedule 1 start-time now life forever</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

8.22 threshold

	Use this command to configure the upper threshold value for IP RNS probe.
	Use the no form of this command to restore the default setting.
	threshold <i>milliseconds</i>
	no threshold

Parameter Description	Parameter	Description
	<i>milliseconds</i>	Sets the upper threshold value, in the range from 0 to 60,000 in the unit of milliseconds.
Defaults	The default is 5,000 milliseconds.	
Command Mode	IP RNS DNS configuration mode IP RNS ICMP echo configuration mode IP RNS TCP configuration mode	
Usage Guide	The threshold value must be no greater than the timeout value. See Usage Guide of the frequency command for the relationship among timeout, frequency and threshold.	
Configuration Examples	The following example sets the upper threshold value for IP RNS probe to 8,000 milliseconds. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# threshold 8000 FS(config-ip-rns-icmp-echo)# exit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.23 timeout

	Use this command to set the timeout time of an IP RNS probe. Use the no form of this command to restore the default setting.	
	timeout <i>milliseconds</i>	
	no timeout	
Parameter Description	Parameter	Description
	<i>milliseconds</i>	Sets the timeout time, in the range from 10 to 604,800,000 in the unit of milliseconds. The default is 5,000 milliseconds.
Defaults	The default timeout of an IP RNS probe varies with the detection type, which can be displayed by using show ip rns configuration command.	
Command Mode	IP RNS ICMP echo configuration mode IP RNS DNS configuration mode	

	IP RNS TCP configuration mode	
Usage Guide	The timeout value must be no smaller than the threshold value. See Usage Guide of the frequency command for the relationship among timeout, frequency and threshold.	
Configuration Examples	The following example sets the timeout time of an IP RNS probe to 10,000 milliseconds. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# timeout 10000 FS(config-ip-rns-icmp-echo)# exit</pre>	
Related Commands	Command	Description
	frequency <i>milliseconds</i>	Sets the interval of sending the packets.
Platform Description	N/A	

8.24 tos

	Use this command to set the Type of Service (ToS) field in the IPv4 header of an IP RNS probe packet. Use the no form of this command to restore the default setting.	
	tos <i>number</i>	
	no tos	
Parameter Description	Parameter	Description
	<i>number</i>	Sets the ToS field in the IPv4 header of an IP RNS probe packet, in the range from 0 to 255.
Defaults	The default is 0.	
Command Mode	IP RNS DNS configuration mode IP RNS ICMP echo configuration mode IP RNS TCP configuration mode	
Usage Guide	ToS is an 8-bit field of an IPv4 packet. ToS can be used to set probe packet priority. Different ToS corresponds to different priority.	
Configuration Examples	The following example sets the ToS field in the IPv4 header of an IP RNS probe packet to 128. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 10.1.1.1 FS(config-ip-rns-icmp-echo)# tos 128 FS(config-ip-rns-icmp-echo)# exit</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.25 track interface line-protocol

	Use this command to configure a tracked object to track the interface status and enter the track mode. Use the no form of this command to delete a tracked object.	
	track <i>object-number</i> interface <i>interface-type</i> <i>interface-number</i> line-protocol	
	no track <i>object-number</i>	
Parameter Description	Parameter	Description
	<i>object-number</i>	Sets the tracked object number, in the range of 1 to 700.
	<i>interface-type</i> <i>interface-number</i>	Sets the interface type and the interface number.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure a tracked object to track the link state of the interface. If the link state of the interface is up, the state of the corresponding tracked object is up too.	
Configuration Examples	The following example configures the object "track 3" to track the link state of ethernet 0/1. FS(config)# track 3 interface ethernet 0/1 line-protocol	
Related Commands	Command	Description
	track rns	Configures a tracked object to track the operating status of an rns object.
	show track	Displays the tracked object related information.
Platform Description	N/A	

8.26 track list

	Use this command to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation.

	Use the no form of this command to restore the default setting.	
	track <i>object-number</i> list boolean { and or }	
	no track <i>object-number</i>	
Parameter Description	Parameter	Description
	<i>object-number</i>	Sets the number of the tracked object, in the range from 1 to 700.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure a tracked list object and specify the state of the tracked list based on a Boolean calculation ● track <i>object-number</i> list boolean and: Configure a tracked list with a Boolean expression using “AND” operator. ● track <i>object-number</i> list boolean or: Configure a tracked list with a Boolean expression using “OR” operator.	
Configuration Examples	The following example configures tracked list object “4” and specifies the state of the tracked list based on a Boolean calculation using operator “AND”. <pre>FS(config)# track 4 list boolean and</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.27 track rns

	Use this command to configure a tracked object to track the operating status of an RNS object and enter the track mode. Use the no form of this command is used to delete a tracked object.	
	track <i>object-number</i> rns entry-number	
	no track <i>object-number</i>	
Parameter Description	Parameter	Description
	<i>object-number</i>	Sets the tracked object number, in the range from 1 to 700.
	<i>entry-number</i>	Sets the RNS object number, in the range from 1 to 500.

Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	The RNS object status is determined by whether the response packets are received. If so, the RNS object status is up and the status of the corresponding tracked object that tracks this RNS is also up.	
Configuration Examples	The following example configures the object "track 5" to track the RNS instance "rns 7". <pre>FS(config)# track 5 rns 7</pre>	
Related Commands	Command	Description
	track interface line-protocol	Tracks the status of one interface and enter the track mode.
	show track [track-number]	Displays the tracked object related information.
Platform Description	N/A	

8.28 track rns-list

	Use this command to configure a tracked object to track the detection result of an RNS list instance. Use the no form of this command to delete a tracked object. track object-number rns-list men-list { and or } no track object-number	
Parameter Description	Parameter	Description
	object-number	Indicates the number of the tracked object. The value ranges from 1 to 700.
	men-list	Indicates the RNS list to be tracked. The value can be an RNS detection instance or a range of RNS detection instances. The instance range begins with a smaller RNS ID, ends with a larger RNS ID and is separated with an en dash (-), for example, 10-20. The value of an RNS ID ranges from 1 to 500.
Defaults	N/A	
Command Mode	Global configuration mode	
Default Level	1	
Usage Guide	This command is used to configure a tracked object and specify the status of an RNS list based on a Boolean calculation. track object-number rns-list men-list and: Configures a tracked object to track the status of a tracked list	

	with a Boolean expression using the "AND" operator. ● track object-number rns-list men-list or: Configures a tracked object to track the status of an RNS list with a Boolean expression using the "OR" operator.
Configuration Examples	The following example configures tracked object numbered 5 to track RNS instances numbered 1, 2–5, and 8. <pre>FS(config)# track 5 rns-list 1,2-5,8 and</pre>
Verification	Run the show track command to display statistics of the tracked object.
Prompts	1. If resources on the device are insufficient when a tracked object is configured, an error will be displayed. <pre>Failed to create track obj, no resource.</pre> 2. If the no track command is executed to delete a specified tracked object but this object does not exist on the device, an error will be displayed. <pre>the track object does not exist.</pre>
Common Errors	1. A tracked object is configured to track an RNS list but the relevant RNS instance is not configured.
Platform Description	N/A

8.29 vrf

	Use this command to set the VRF where the IP RNS probe resides. Use the no form of this command to restore the default setting.	
	vrf vrf-name no vrf	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	Sets the VRF name.
Defaults	N/A	
Command Mode	IP RNS ICMP echo configuration mode IP RNS DNS configuration mode IP RNS TCP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the VRF where the IP RNS probe resides to VPN1. <pre>FS(config)# ip rns 1 FS(config-ip-rns)# icmp-echo 192.168.23.1 FS(config-ip-rns-icmp-echo)# vrf VPN1</pre>	

	FS(config-ip-rns-icmp-echo)# exit FS(config)# ip rns schedule 1 start-time now life forever	
Related Commands	Command	Description
	frequency <i>milliseconds</i>	Sets the interval of sending the packets.
Platform Description	N/A	

System Configuration Commands

1 Command Line Interface Commands

1.1 alias

	Use this command to configure a command alias in global configuration mode. Use the no or default form of this command to restore the default setting.													
	alias <i>mode command-alias original-command</i>													
	no alias <i>mode [command-alias]</i> default alias mode <i>[command-alias]</i>													
Parameter Description	Parameter	Description												
	<i>mode</i>	Mode of the command represented by the alias												
	<i>command-alias</i>	Command alias												
	<i>original-command</i>	Syntax of the command represented by the alias												
Defaults	Some commands in user or privileged EXEC mode have default alias.													
Command Mode	Global configuration mode.													
Usage Guide	The following table lists the default alias of the commands in privileged EXEC mode. <table><tr><th>Alias</th><th>Actual Command</th></tr><tr><td>h</td><td>help</td></tr><tr><td>p</td><td>ping</td></tr><tr><td>s</td><td>show</td></tr><tr><td>u</td><td>undebug</td></tr><tr><td>un</td><td>undebug</td></tr></table> The default alias cannot be removed by the no alias exec command. After configuring the alias, you can use a word to replace a command. For example, you can create an alias to represent the first part of a command, and then type the rest part of the command. The mode of the command represented by the alias is the command mode existing in the current system. In the global configuration mode, you can use the alias ? command to list all the modes under which you can configure alias for commands. <pre>FS(config)# alias ? aaa-gs AAA server group mode acl acl configure mode bgp Configure bgp Protocol config goble configure mode</pre>		Alias	Actual Command	h	help	p	ping	s	show	u	undebug	un	undebug
Alias	Actual Command													
h	help													
p	ping													
s	show													
u	undebug													
un	undebug													

	 The alias also has its help information that is displayed after * in the following format: <pre>*command-alias=original-command</pre> For example, in the privileged EXEC mode, the default alias s stands for show. You can enter s? to query the key words beginning with s and the help information of the alias. <pre>FS#s?</pre> <pre>*s=show show start-chat start-terminal-service</pre> If an alias represents more than one word, the command will be displayed in brackets. For example, if you set sv stand for show version in the privileged EXEC mode, then: <pre>FS#s?</pre> <pre>*s=show *sv="show version" show start-chat</pre> <pre>start-terminal-service</pre> The alias must begin with the first letter of the command. The first letter of the command cannot be a space. The space before the command cannot be used as a valid alias. <pre>FS# s?</pre> <pre>show start-chat start-terminal-service</pre> The command alias also has its help information. For example, if the alias ia represents ip address in the interface configuration mode, then: <pre>FS(config-if)#ia ?</pre> <pre> A.B.C.D IP address</pre> <pre> dhcp IP Address via DHCP</pre> <pre>FS(config-if)# ip address</pre> The above help information lists the parameters of ip address and shows the actual command name. You must enter an entire alias; otherwise it cannot be recognized. Use the show aliases command to show the aliases setting in the system.	
Configuration Examples	The following example uses def-route to represent the default route setting of ip route 0.0.0.0 0.0.0.0 192.168.1.1 in the global configuration mode: <pre>FS# configure terminal</pre> <pre>FS(config)# alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre> <pre>FS(config)#def-route?</pre> <pre>*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"</pre> <pre>FS(config)# end</pre> <pre>FS# show aliases config</pre> <pre>globe configure mode alias:</pre> <pre>def-route ip route 0.0.0.0 0.0.0.0</pre> <pre>192.168.1.1</pre>	
Related Commands	Command	Description
	show aliases	Displays the aliases settings.
Platform Description	N/A	

1.2 cli-python

	Use this command to install and uninstall a python script for CLI.	
	cli-python { insmod rmmmod } python-filename	
Parameter Description	Parameter	Description
	<i>python-filename</i>	Python script filename.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	Upload a python script to the flash directory and run this command to install the python script.	
Configuration Examples	The following example installs python script FS.py. <pre>FS# cli-python insmod FS.py</pre> % Python script module "FS.py" insert success.	
Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

1.3 privilege

	Use this command to attribute the execution rights of a command to a command level in global configuration mode. Use the no form of this command to restore the default setting.	
	privilege mode [all] [level level reset] command-string	
	no privilege mode [all] [level level] command-string	
Parameter Description	Parameter	Description
	<i>mode</i>	CLI mode of the command to which the execution rights are attributed.
	all	Command alias
	level level	Specifies the execution right levels (0–15) of a command or sub-commands
	reset	Restores the command execution rights to its default level
	<i>command-string:</i>	Command string to be authorized
Defaults	N/A	

Command Mode	Global configuration mode.																	
Usage Guide	The following table lists some key words that can be authorized by the privilege command in CLI mode. The number of command modes that can be authorized may vary with different devices. In the global configuration mode, you can use the privilege ? command to list all CLI command modes that can be authorized. <table><tr><th>Mode</th><th>Description</th></tr><tr><td>config</td><td>Global configuration mode.</td></tr><tr><td>exec</td><td>Privileged EXEC mode</td></tr><tr><td>interface</td><td>Interface configuration mode</td></tr><tr><td>ip-dhcp-pool</td><td>DHCP address pool configuration mode</td></tr><tr><td>ip-dhcp-pool</td><td>DHCP address pool configuration mode</td></tr><tr><td>keychain</td><td>KeyChain configuration mode</td></tr><tr><td>keychain-key</td><td>KeyChain-key configuration mode</td></tr></table>		Mode	Description	config	Global configuration mode.	exec	Privileged EXEC mode	interface	Interface configuration mode	ip-dhcp-pool	DHCP address pool configuration mode	ip-dhcp-pool	DHCP address pool configuration mode	keychain	KeyChain configuration mode	keychain-key	KeyChain-key configuration mode
Mode	Description																	
config	Global configuration mode.																	
exec	Privileged EXEC mode																	
interface	Interface configuration mode																	
ip-dhcp-pool	DHCP address pool configuration mode																	
ip-dhcp-pool	DHCP address pool configuration mode																	
keychain	KeyChain configuration mode																	
keychain-key	KeyChain-key configuration mode																	
Configuration Examples	The following example sets the password of CLI level 1 as test and attribute the reload rights to reset the device: <pre>FS(config)#privilege exec level 1 reload</pre> You can access the CLI window as level-1 user to use the reload command: <pre>FS>reload ?</pre> <pre>LINE Reason for reload</pre> <cr> You can use the key word all to attribute all sub-commands of reload to level-1 users: <pre>FS(config)# privilege exec all level 1 reload</pre> After the above setting, you can access the CLI window as level-1 user to use all sub commands of the reload command: <pre>FS>reload ?</pre> <pre>LINE Reason for reload</pre> <pre>at reload at a specific time/date</pre> <pre>cancel cancel pending reload scheme</pre> <pre>in reload after a time interval</pre> <pre><cr></pre>																	
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>enable secret</td><td>Sets the CLI-level password.</td></tr></table>	Command	Description	enable secret	Sets the CLI-level password.													
Command	Description																	
enable secret	Sets the CLI-level password.																	
Platform Description	N/A.																	

1.4 show aliases

	Use this command to show all the command aliases or aliases in special command modes.
	show aliases [mode]

Parameter Description	Parameter	Description
	<i>mode</i>	Mode of the command represented by the alias.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	This command displays the configuration of all aliases if no command mode is input.	
Configuration Examples	The following example displays the command alias in privileged EXEC mode: <pre>FS#show aliases exec exec mode alias: h help p ping s show u undebug un undebug</pre>	
Related Commands	Command	Description
	alias	Sets a command alias.
Platform Description	N/A.	

2 Basic Configuration Management Commands

2.1 <1-99>

	Use this command to restore the suspended Telnet Client session.	
	<1-99>	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	This command is used to restore the suspended Telnet Client session. Hot keys (ctrl+shift+6 x) are used to exit the Telnet Client session creation. The <1-99> command is used to restore the session. If the session is created, you can use the show session command to display the session.	
Configuration Examples	The following example restores the suspended Telnet Client session. FS# 1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.2 banner exec

	Use this command to configure a message to welcome the user entering user EXEC mode through the line. Use the no form of this command to restore the default setting.	
	banner exec c message c	
	no banner exec	
Parameter Description	Parameter	Description
	c	Separator of the message. Delimiters are not allowed in the message.
	message	Contents of the message.
Defaults	N/A	

Command Mode	Global configuration mode	
Usage Guide	This command is used to configure the welcome message. The system discards all the characters next to the terminating symbol. When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the EXEC message or the incoming message is displayed. If it's a reverse Telnet session, the incoming message is displayed. Otherwise, the EXEC message is displayed. The messages are for all lines. If you want to disable display the EXEC message on a specific line, configure the no exec-banner command on the line.	
Configuration Examples	The following example configures a welcome message. <pre>FS(config)# banner exec \$ Welcome \$</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.3 banner incoming

	Use this command to configure a prompt message for reverse Telnet session. Use the no form of this command to remove the setting.	
	banner incoming <i>c message c</i>	
	no banner incoming	
Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
	<i>message</i>	Contents of the message.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure a prompt message. The system discards all the characters next to the terminating symbol. When you are logging in to the device, the MOTD message is displayed at first, and then the banner login message. After you have logged in, the welcome message or the prompt message is displayed. If it's a reverse Telnet session, the prompt message is displayed. Otherwise, the welcome message is displayed.	

Configuration	The following example configures a prompt message for reverse Telnet session.	
Examples	FS(config)# banner incoming \$ Welcome \$	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.4 banner login

	Use this command to configure a login banner. Use no form of this command to r remove the setting.	
	banner login <i>c message c</i>	
	no banner login	
Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message contained in the login banner. Delimiters are not allowed in the MOTD.
	<i>message</i>	Contents of the login banner
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command sets the login banner message, which is displayed at login. The system discards all the characters next to the terminating symbol.	
Configuration Examples	The following example configures a login banner. FS(config)# banner login \$ enter your password \$	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.5 banner motd

	Use this command to set the Message-of-the-Day (MOTD) . Use the no form of this command to remove the setting.	
	banner [motd] c message c	
	no banner [motd]	
Parameter Description	Parameter	Description
	<i>c</i>	Separator of the MOTD. Delimiters are not allowed in the MOTD.
	<i>message</i>	Contents of an MOTD
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command sets the MOTD, which is displayed at login. The letters that follow the separator will be discarded.	
Configuration Examples	The following example configures the MOTD. FS(config)# banner motd \$ hello,world \$	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.6 banner prompt-timeout

	Use this command to configure the prompt-timeout message to notify timeout. Use the no form of this command to remove the setting.	
	banner prompt-timeout c message c	
	no banner prompt-timeout	
Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
	<i>message</i>	Contents of the message.
Defaults	N/A	
Command	Global configuration mode	

Mode		
Usage Guide	The system discards all the characters next to the terminating symbol. When authentication times out, the banner prompt-timeout message is displayed.	
Configuration Examples	The following example configures the prompt-timeout message to notify timeout. <pre>FS(config)# banner exec \$ authentication timeout \$</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.7 banner slip-ppp

	Use this command to configure the slip-ppp message for the SLIP/PPP session. Use the no form of this command to remove the setting.	
	banner slip-ppp <i>c message c</i>	
	no banner slip-pp	
Parameter Description	Parameter	Description
	<i>c</i>	Separator of the message. Delimiters are not allowed in the message.
	<i>message</i>	Contents of the message.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure the slip-ppp message for the SLIP/PPP session. The system discards all the characters next to the terminating symbol. When the SLIP/PPP session is created, the slip-ppp message is displayed on the corresponding terminal.	
Configuration Examples	The following example configures the banner slip-ppp message for the SLIP/PPP session. <pre>FS(config)# banner slip-ppp \$ Welcome \$</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

2.8 boot config

	Use this command to modify the path for saving startup configurations and the corresponding file name.	
	boot config { flash:filename usb0:filename }	
	no boot config	
Parameter Description	Parameter	Description
	flash	Saves the startup configuration file in the extensible Flash.
	usb0	Saves the startup configuration file in USB0 device. The device must have a USB interface into which a USB device is inserted.
Defaults	By default, startup configuration file of a device is saved in Flash:/config.text	
Command Mode	Privileged EXEC mode	
Usage Guide	 The startup configuration file name follows a slash "/", for example, Flash:/FS.text and Usb0:/FS.text.  The startup configuration file name consists of a path and a file name. The path is mandatory. Otherwise, configurations cannot be saved by using the write command. Take Flash:/FS/FS.text and Usb0:/FS/FS.text as examples, where the Flash:/FS and Usb0:/FS folders must exist. In master-slave mode, all device paths are required.  To save the startup configuration file to a USB flash drive, the device must provide a USB interface with a USB flash drive inserted. Otherwise, configurations cannot be saved by using the write command. In master-slave mode, all devices must have USB flash drives connected.	
Configuration Examples	The following example sets the startup configuration file path to flash:/FS.text.. <pre>FS(config)#boot config flash:/FS.text</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.9 configure

	Use this command to enter global configuration mode.
	configure [terminal]

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example enters global configuration mode. FS# configure FS(config)#	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.10 disable

	Use this command to switch from privileged EXEC mode to user EXEC mode or lower the privilege level.	
	disable [<i>privilege-level</i>]	
Parameter Description	Parameter	Description
	privilege-level	Privilege level
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	Use this command to switch to user EXEC mode from privileged EXEC mode. If a new privilege level is added, the current privilege level will be lowered.  The privilege level that follows the disable command must be lower than the current level.	
Configuration	The following example lowers the current privilege level of the device to level 10.	

Examples	FS# disable 10	
Related Commands	Command	Description
	enable	Moves from user EXEC mode enter to privileged EXEC mode or reaches a higher level of authority.
Platform Description	N/A	

2.11 disconnect

	Use this command to disconnect the Telnet Client session.	
	disconnect <i>session-id</i>	
Parameter Description	Parameter	Description
	<i>session-id</i>	Telnet Client session ID.
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	This command is used to disconnect the Telnet Client session by setting the session ID.	
Configuration Examples	The following example disconnects the Telnet Client session by setting the session ID. FS# disconnect 1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.12 do telnet

	Use this command to login to Telnet server.
	do telnet [oob] <i>host</i> [<i>port</i>] [/ source { ip <i>A.B.C.D</i> ipv6 <i>X:X:X::X</i> interface <i>interface-name</i> }] [/ vrf <i>vrf-name</i>] [via <i>mgmt-name</i>]

Parameter Description	Parameter	Description
	oob	Connects to Telnet server through oob channel. This parameter is available only when the device has a MGMT port.
	<i>host</i>	IPv4, IPv6 or host name of Telnet server.
	<i>port</i>	Configures TCP port ID. The default is 23.
	/source	Specifies source IP or source port for Telnet client.
	ip <i>A.B.C.D</i>	Specifies source IPv4 address for Telnet client.
	ipv6 <i>X:X:X:X::X</i>	Specifies source IPv6 address for Telnet client.
	interface <i>interface-name</i>	Specifies source port for Telnet client.
	/vrf <i>vrf-name</i>	Specifies VRF table.
	via <i>mgmt-name</i>	Specifies MGMT table.
Defaults	N/A	
Command Mode	User EXEC mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example configures destination IPv4 address 192.168.1.1, uses default port ID, and specifies source port Gi 0/1 and VRF table vpn1. <pre>FS(config)# do telnet 192.168.1.1 /source interface gigabitEthernet 0/1 /vrf vpn1</pre> The following example configures destination IPv6 address 2AAA:BBBB::CCCC. <pre>FS(config)# do telnet 2AAA:BBBB::CCCC</pre> The following example configures destination IPv4 address 192.168.1.1 and specifies MGMT port Mgmt 0. <pre>FS(config)# do telnet oob 192.168.1.1 via mgmt 0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.13 enable

	Use this command to enter privileged EXEC mode.	
	Enable [<i>privilege-level</i>]	
Parameter Description	Parameter	Description
	<i>privilege-level</i>	Privilege level

Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example enters privileged EXEC mode and lowers the privilege level to 14. <pre>FS> enable 14</pre> Password:	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.14 enable password

	Use this command to configure passwords for different privilege levels. Use the no form of this command to restore the default setting.	
	enable password [<i>level level</i>] { [0] <i>password</i> 7 <i>encrypted-password</i> }	
	no enable password [<i>level level</i>]	
Parameter Description	Parameter	Description
	<i>password</i>	Password for the user to enter the EXEC configuration layer
	<i>level</i>	User's level.
	0	(Optional) The password is in plain text.
	7 <i>encrypted-password</i>	The password is encrypted.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	No encryption is required in general. The encryption type must be specified for copying and pasting a encrypted password for the device. A valid password is defined as follows: ● Consists of 1-26 upper/lower case letters and numbers ● Leading spaces are allowed but usually ignored. Spaces in between or at the end are regarded as part of the	

	password.	
	 If an encryption type is specified and a plaintext password is entered, you cannot enter privileged EXEC mode. A lost password that has been encrypted using any method cannot be restored. In this case, you can only reconfigure the device password.	
Configuration Examples	The following example configures the password as pw10 . <pre>FS(config)# enable password pw10</pre>	
Related Commands	Command	Description
	enable secret	Sets the security password
Platform Description	N/A	

2.15 enable secret

	Use this command to configure a security password for different privilege levels. Use the no form of this command to restore the default setting.	
	enable secret [<i>level level</i>] { [0] <i>password</i> 5 encrypted-secret }	
	no enable secret [<i>level level</i>]	
Parameter Description	Parameter	Description
	secret	Password for the user to enter the EXEC configuration layer
	level	User's level.
	0	"0" for no encryption.
	5 encrypted-password	"5" for security encryption.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	A password comes under two categories: "password" and "security". "Password" indicates a simple password, which can be set only for level 15. "Security" means a security password, which can be set for levels 0-15. If both types of passwords coexist in the system, no "password" type is allowed. If a "password" type password is set for a level other than 15, the system gives an alert and the password is automatically converted into a "security" password. If a "password" type password is set for level 15 and the same as a "security" password, an alert is given. The password must be encrypted, with simple encryption for "password" type passwords and security encryption for "security" type passwords.	

Configuration Examples	The following example configures the security password as pw10 . FS(config)# enable secret 0 pw10	
Related Commands	Command	Description
	enable password	Sets passwords for different privilege levels.
Platform Description	N/A	

2.16 enable service

	Use this command to enable or disable a specified service such as SSH Server/Telnet Server/Web Server/SNMP Agent .	
	enable service { ssh-sesrver telnet-server web-server [http https all] snmp-agent }	
Parameter Description	Parameter	Description
	ssh-server	Enables SSH Server. IPv4 and IPv6 services are enabled at the same time.
	telnet-server	Enables Telnet Server. IPv4 and IPv6 services are enabled at the same time.
	web-server [http https all]	Enables HTTP Server. IPv4 and IPv6 services are enabled at the same time.
	snmp-agent	Enables SNMP Agent. IPv4 and IPv6 services are enabled at the same time.
Defaults	telnet-server, snmp-agent and web-server are enabled and ssh-server is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable or disable a specified service. Use the no enable service command to disable the specified service.  The enable service web-server command is followed by three optional keywords: [http https all]. If the command is followed by no keyword or by all, the command enables http and https services. Followed by http, the command enables http service only. Followed by https, the command enables https service only.	
Configuration Examples	The following example enables the SSH Server. FS(Config)# enable service ssh-sesrver	
Related Commands	Command	Description
	show service	Displays the service status in the current system.
Platform	N/A	

Description	

2.17 end

	Use this command to return to privileged EXEC mode.	
	end	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	All modes except privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example returns to privileged EXEC mode. <pre>FS#con Enter configuration commands, one per line. End with CNTL/Z. FS(config)#line vty 0 FS(config-line)#end *May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console FS#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.18 exec-banner

	Use this command to enable display of the EXEC message on a specific line. Use the no form of this command to restore the default setting.	
	exec-banner	
	no exec-banner	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	The EXEC message is displayed on all lines by default.	
Command Mode	LINE configuration mode	
Usage Guide	After you configure the banner exec and the banner motd commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the no form of this command on the line.  This command does not work for the banner incoming message. If you configure the banner incoming command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.	
Configuration Examples	The following example disables display of the EXEC message on line VTY 1. <pre>FS(config)# line vty 1 FS(config-line)no exec-banner</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.19 exec-timeout

	Use this command to configure connection timeout for this device in LINE mode. Use the no form of this command to restore the default setting and the connection never expires.	
	exec-timeout <i>minutes</i> [<i>seconds</i>]	
	no exec-timeout	
Parameter Description	Parameter	Description
	<i>minutes</i>	Timeout in minutes.
	<i>seconds</i>	(Optional) Timeout in minutes
Defaults	The default is 10 minutes.	
Command Mode	Line configuration mode	
Usage Guide	If there is no input or output for this connection within a specified time, this connection will expire, and this LINE will be restored to the free status.	

Configuration Examples	The following example sets the connection timeout to 5'30". <code>FS(config-line)#exec-timeout 5 30</code>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.20 execute

	Use this command to execute a command on the file.	
	execute { [flash:] <i>filename</i> }	
Parameter Description	Parameter	Description
	<i>filename</i>	Specifies the file path.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example executes a command to configure an IP address for the specified interface. <pre> FS#execute flash:mybin/config.text executing script file mybin/config.text executing done FS#config Enter configuration commands, one per line. End with CNTL/Z. FS(config)#interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#ip address 192.168.21.158 24 FS(config-if-GigabitEthernet 0/1)#end *Sep 29 23:35:49: %SYS-5-CONFIG_I: Configured from console by console FS# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.21 exit

	Use this command to return to the upper configuration mode.	
	exit	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	All configuration modes	
Usage Guide	N/A	
Configuration Examples	The following example returns to the upper configuration mode. <pre> FS#con Enter configuration commands, one per line. End with CNTL/Z. FS(config)#line vty 0 FS(config-line)#end *May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console FS#con Enter configuration commands, one per line. End with CNTL/Z. FS(config)#line vty 0 FS(config-line)#exit FS(config)#exit *May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console FS#exit Press RETURN to get started </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.22 help

	Use this command to display the help information.	
	help	

Parameter Description	Parameter	Description																																
	N/A	N/A																																
Defaults	Any mode																																	
Command Mode																																		
Usage Guide	This command is used to display brief information about the help system. You can use "?" to display all commands or a specified command with its parameters.																																	
Configuration Examples	The following example displays brief information about the help system. <pre>FS#help</pre> Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options. Two styles of help are provided: 1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument. 2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'). The following example displays all available commands in interface configuration mode. <pre>FS(config-if-GigabitEthernet 0/0)#?</pre> Interface configuration commands: <table><tr><td>arp</td><td>ARP interface subcommands</td></tr><tr><td>bandwidth</td><td>Set bandwidth informational parameter</td></tr><tr><td>carrier-delay</td><td>Specify delay for interface transitions</td></tr><tr><td>dampening</td><td>Enable event dampening</td></tr><tr><td>default</td><td>Set a command to its defaults</td></tr><tr><td>description</td><td>Interface specific description</td></tr><tr><td>dldp</td><td>Exec data link detection command</td></tr><tr><td>duplex</td><td>Configure duplex operation</td></tr><tr><td>efm</td><td>Config efm for an interface</td></tr><tr><td>end</td><td>Exit from interface configuration mode</td></tr><tr><td>exit</td><td>Exit from interface configuration mode</td></tr><tr><td>expert</td><td>Expert extended ACL</td></tr><tr><td>flowcontrol</td><td>Set the flow-control value for an interface</td></tr><tr><td>full-duplex</td><td>Force full duplex operation</td></tr><tr><td>global</td><td>Global ACL</td></tr><tr><td>gvrp</td><td>GVRP configure command</td></tr></table>		arp	ARP interface subcommands	bandwidth	Set bandwidth informational parameter	carrier-delay	Specify delay for interface transitions	dampening	Enable event dampening	default	Set a command to its defaults	description	Interface specific description	dldp	Exec data link detection command	duplex	Configure duplex operation	efm	Config efm for an interface	end	Exit from interface configuration mode	exit	Exit from interface configuration mode	expert	Expert extended ACL	flowcontrol	Set the flow-control value for an interface	full-duplex	Force full duplex operation	global	Global ACL	gvrp	GVRP configure command
arp	ARP interface subcommands																																	
bandwidth	Set bandwidth informational parameter																																	
carrier-delay	Specify delay for interface transitions																																	
dampening	Enable event dampening																																	
default	Set a command to its defaults																																	
description	Interface specific description																																	
dldp	Exec data link detection command																																	
duplex	Configure duplex operation																																	
efm	Config efm for an interface																																	
end	Exit from interface configuration mode																																	
exit	Exit from interface configuration mode																																	
expert	Expert extended ACL																																	
flowcontrol	Set the flow-control value for an interface																																	
full-duplex	Force full duplex operation																																	
global	Global ACL																																	
gvrp	GVRP configure command																																	

	half-duplex Force half duplex operation help Description of the interactive help system ip Interface Internet Protocol config commands ipv6 Internet Protocol Version 6 isis Intermediate System - Intermediate System (IS-IS) l2 Config L2 attribute label-switching Enable interface process mpls packet lACP LACP interface subcommands lldp Link Layer Discovery Protocol load-interval Specify interval for load calculation for an interface mac Mac extended ACL mac-address Set mac-address mpls Multi-Protocol Label Switching mtu Set the interface Maximum Transmission Unit (MTU) no Negate a command or set its defaults ntp Configure NTP port-group Aggregateport/port bundling configuration redirect Redirect packets rmon Rmon command security Configure the Security show Show running system information shutdown Shutdown the selected interface snmp Modify SNMP interface parameters speed Configure speed operation switchport Set switching mode characteristics vrf Multi-af VPN Routing/Forwarding parameters on the interface vrrp VRRP interface subcommands xconnect Xconnect commands The following example displays the parameters of a specified command. <pre>FS(config)#access-list 1 permit ? A.B.C.D Source address any Any source host host A single source host</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

2.23 hostname

	Use this command to specify or modify the hostname of a device.

	hostname <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Device hostname, string, number or hyphen, up to 63 characters.
Defaults	The default is FS.	
Command Mode	Global configuration mode	
Usage Guide	This hostname is mainly used to identify the device and is taken as the username for the local device during dialup and CHAP authentication.	
Configuration Examples	The following example configures the hostname of the device as BeiJingAgenda. <pre>FS(config)# hostname BeiJingAgenda BeiJingAgenda(config)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.24 ip telnet source-interface

	Use this command to configure the IP address of an interface as the source address for Telnet connection.	
	ip telnet source-interface <i>interface-name</i>	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Configures the IP address of the interface as the source address for Telnet connection.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to specify the IP address of an interface as the source address for global Telnet connection. When using the telnet command to log in a Telnet server, apply the global setting if no source interface or source address is specified. Use the no ip telnet source-interface command to restore it to the default setting.	

Configuration Examples	The following example configures the IP address of the <i>Loopback1</i> interface as the source address for global Telnet connection.	
	FS(Config)# ip telnet source-interface Loopback 1	
Related Commands	Command	Description
	telnet	Logs in a Telnet server.
Platform Description	N/A	

2.25 language character-set

	Use this command to set a language character set.	
	language character-set { UTF-8 GBK default }	
Parameter Description	Parameter	Description
	UTF-8	Specifies the UTF-8 character set.
	GBK	Specifies the GBK character set.
	default	Specifies the default character set.
Defaults	Default	
Command Mode	Global configuration mode	
Usage Guide	If you want to set a character set in running configuration, please delete the character set configuration different from the target character set first.	
Configuration Examples	The following example specifies the UTF-8 character set.	
	FS(config)#language character-set UTF-8 This may take some time to build configuration, Continue? (yes[no]): y FS(config)#	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.26 lock

	Use this command to set a temporary password for the terminal.	
	lock	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	You can lock the terminal interface and maintain the session continuity to prevent access to the interface by setting a temporary password. Take the following steps to lock the terminal interface: ● Enter the lock command, and the system will prompt you for a password: ● Enter the password, which can be any character string. The system will prompt you to confirm the password, clear the screen, and display the "Locked" information. ● To access the terminal, enter the preset temporary password. ● To lock the terminal, run the lockable command in line configuration mode and enable terminal locking in the corresponding line.	
Configuration Examples	The following example locks a terminal interface. <pre>FS(config-line)# lockable FS(config-line)# end FS# lock Password: <password> Again: <password> Locked Password: <password> FS#</pre>	
Related Commands	Command	Description
	lockable	Supports terminal locking in the line.
Platform Description	N/A	

2.27 lockable

	Use this command to support the lock command at the terminal. Use the no form of this command to restore the default setting.

	lockable	
	no lockable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default	
Command Mode	Line configuration mode	
Usage Guide	This command is used to lock a terminal interface in the corresponding line. To lock the terminal, run the lock command in EXEC mode.	
Configuration Examples	The following example enables terminal locking at the console port and locks the console. <pre> FS(config)# line console 0 FS(config-line)# lockable FS(config-line)# end FS# lock Password: <password> Again: <password> Locked Password: <password> </pre>	
Related Commands	Command	Description
	lock	Locks the terminal.
Platform Description	N/A	

2.28 login

	Use this command to enable simple login password authentication on the interface if AAA is disabled. Use the no form of this command to restore the default setting.	
	login	
	no login	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Login is disabled for console and enabled for AUX, TTY and VTY terminals by default.	

Command Mode	Line configuration mode	
Usage Guide	If the AAA security server is inactive, this command enables simple password authentication at login. The password is configured for a VTY or console interface.	
Configuration Examples	The following example sets a login password authentication on VTY.. FS(config)# no aaa new-model FS(config)# line vty 0 FS(config-line)# password 0 normatest FS(config-line)# login	
Related Commands	Command	Description
	password	Configures the line login password
Platform Description	N/A	

2.29 login access non-aaa

	Use this command to configure non-AAA authentication on line when AAA is enabled. Use the no form of this command to restore the default setting.	
	login access non-aaa	
	no login access non-aaa	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example configures VTY line authentication with AAA enabled. FS(config)#log access non-aaa FS(config)#aaa new-model FS(config)#line vty 0 4 FS(config-line)#login local FS(config-line)#	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.30 login authentication

	If the AAA is enabled, login authentication must be performed on the AAA server. Use this command to associate login authentication method list. Use the no form of this command to remove the configuration.	
	login authentication { default <i>list-name</i> }	
	no login authentication { default <i>list-name</i> }	
Parameter Description	Parameter	Description
	default	Name of the default authentication method list
	<i>list-name</i>	Name of the method list
Defaults	The default authentication is used when AAA is enabled.	
Command Mode	Line configuration mode	
Usage Guide		
Configuration Examples	The following example associates the method list on VTY and perform login authentication on a radius server. <pre>FS(config)# aaa new-model FS(config)# aaa authentication login default radius FS(config)# line vty 0 FS(config-line)# login authentication default</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authentication login	Configures the login authentication method list.
Platform Description	N/A	

2.31 login local

	Use this command to enable local user authentication on the interface if AAA is disabled. Use the no form of this command to restore the default setting.	
	login local	
	no login local	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	If the AAA security server is inactive, this command is used for local user login authentication. The user is allowed to use the username command.	
Configuration Examples	The following example sets local user authentication on VTY. <pre> FS(config)# no aaa new-model FS(config)# username test password 0 test FS(config)# line vty 0 FS(config-line)# login local </pre>	
Related Commands	Command	Description
	username	Configures local user information.
Platform Description	N/A	

2.32 login privilege log

	Use this command to log privilege change. Use the no form of this command to restore the default setting.	
	login privilege log	
	no login privilege log	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This command is disabled by default.	

Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the function of logging privilege change.	
	FS(config)# login privilege log	
	The following example displays the log of privilege change failure.	
	FS>enable 10 Password: Password: Password: % Access denied FS> *Sep 10 11:34:19: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 10 from console failed	
	The following example displays the log of privilege change success.	
	FS>enable 10 Password: FS# *Sep 10 11:34:20: %SYS-5-PRIV_AUTH_SUCCESS: Authentication to privilege level 10 from console success	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.33 motd-banner

	Use this command to enable display of the MOTD message on a specified line. Use the no form of this command to restore the default setting.
	motd-banner
	no motd-banner

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The MOTD message is displayed on all lines by default.	
Command Mode	Line configuration mode	
Usage Guide	After you configure the banner exec and the banner motd commands, the EXEC and the MOTD messages are displayed on all lines by default. If you want to disable display of the EXEC and the MOTD messages on a specific line, configure the no form of this command on the line.  This command does not work for the incoming message. If you configure the banner incoming command, the banner incoming message is displayed on all reverse Telnet sessions and the display cannot be disabled on a specific line.	
Configuration Examples	The following example disables display of the MOTD message on VTY 1. <pre>FS(config)# line vty 1 FS(config-line)no motd-banner</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.34 password

	Use this command to configure a password for line login, run the password command. Use the no form of this command to restore the default setting.	
	password { [0] <i>password</i> 7 <i>encrypted-password</i> }	
	no password	
Parameter Description	Parameter	Description
	<i>password</i>	Password for remote line login
	0	(Optional) The password is in plain text by a FS device.
	7 <i>encrypted-password</i>	The password is encrypted
Defaults	N/A	

Command Mode	Line configuration mode	
Usage Guide		
Configuration Examples	The following example configures the line login password as "red". FS(config)# line vty 0 FS(config-line)# password red	
Related Commands	Command	Description
	login	Moves from user EXEC mode to privileged EXEC mode or enables a higher level of authority.
Platform Description	N/A	

2.35 prompt

	Use this command to set the prompt command. Use the no form of this command to restore the default setting.	
	prompt <i>string</i> no prompt	
Parameter Description	Parameter	Description
	<i>string</i>	Character string of the prompt command, containing up to 32 letters.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If no prompt string is configured, the system name applies and varies with the system name. The prompt command is valid only in EXEC mode.	
Configuration Examples	The following example sets the prompt string to rgnos. FS(config)# prompt rgnos FS(config)# end FSOS	
Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

2.36 secret

	Use this command to set a password encrypted by irreversible MD5 for line login. Use the no form of this command to restore the default setting.	
	secret { [0] <i>password</i> 5 <i>encrypted-secret</i> }	
	no secret	
Parameter Description	Parameter	Description
	0	(Optional) sets the plaintext password text and encrypts it with irreversible MD5 after configuration.
	<i>password</i>	Sets the password plaintext, a string ranging from 1 to 25 characters.
	5 <i>encrypted-secret</i>	Sets the password text encrypted by irreversible MD5 and saves it as the encrypted password after configuration.
Defaults	N/A	
Command mode	Line configuration mode	
Usage Guide	This command is used to set a password encrypted by irreversible MD5 that is authenticated by a remote user through line login.  If the specified encryption type is 5, the logical length of the cipher text to be entered must be 24 and the 1st, 3rd and 8th characters of the password text must be \$. In general, the encryption type does not need to be specified as 5 except when the encrypted password is copied and pasted. Line mode allows configuration of both “password” and “secret” types passwords at the same time. When the two passwords are the same, the system will send alert notification but the configuration will be permitted. When the system is configured with the two passwords, if the user enters a password that does not match the “secret” type password, it will not continue to match the “password” type password and login fails, enhancing security for the system password.	
Configuration Examples	The following example sets the password encrypted by irreversible MD5 for line login to vty0. <pre>FS(config)# line vty 0 FS(config-line)# secret vty0</pre> The following displays the encryption outcome by running the show command. <pre>secret 5 \$1\$X834\$wvx6y794uAD8svzD</pre>	

Related Commands	Command	Description
	login	Sets simple password authentication on the interface as the login authentication mode
Platform Description	N/A	

2.37 session

	Use this command to connect to another device in stacking multiple-device environment (box-type device).	
	session { master device device-number }	
Parameter Description	Parameter	Description
	master	Configures the slave host to connect with the master host or the slave management module with the master management module.
	device device-number	Sets the device number.
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example configures the slave host to connect with the master host in stacking environment. <pre>FS# session master</pre> The following example connects to device1 through session in stacking multiple-device environment (box-type device). <pre>FS# session device 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.38 session-timeout

	Use this command to configure the session timeout for a remote terminal. Use the no form of this command to restore the default setting and the session never expires.

	session-timeout <i>minutes</i> [output]	
	no session-timeout	
Parameter Description	Parameter	Description
	<i>minutes</i>	Timeout in minutes.
	output	Regards data output as the input to determine whether the session expires.
Defaults	The default timeout is 0.	
Command Mode	LINE configuration mode	
Usage Guide	If no input or output in current LINE mode is found on the remote terminal for the session within a specified time, this connection will expire, and this LINE will be restored to the free status.	
Configuration Examples	The following example specifies the timeout as 5 minutes. FS(config-line)# exec-timeout 5 output	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.39 show boot config

	Use this command to display the path for saving startup configurations and the corresponding file name.	
	show boot config	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the path for saving startup configurations and the corresponding file name..	

	FS#show boot config Boot config file: [flash:/FS.text]	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.40 show debugging

	Use this command to display debugging state.	
	show debugging	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays debugging state.	
	FS#show debugging debug fw-group detect intf-state	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.41 show hostname

	Use this command to display the hostname of a device.
	show hostname

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the hostname of a device. <pre>FS#show hostname FS FS#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.42 show language character-set

	Use this command to display the language character set configuration.	
	show language character-set	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the language character set configuration. <pre>FS#show language character-set Current language character set encode: UTF-8 FS#</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.43 show line

	Use this command to display the configuration of a line.	
	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }	
Parameter Description	Parameter	Description
	console	Displays the configuration of a console line.
	vty	Displays the configuration of a vty line.
	<i>line-num</i>	Number of the line.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide		
Configuration Examples	The following example displays the configuration of a console port. <pre> FS# show line console 0 CON Type speed Overruns * 0 CON 9600 45927 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never History is enabled, history size is 10. Total input: 53564 bytes Total output: 395756 bytes Data overflow: 27697 bytes stop rx interrupt: 0 times </pre>	
Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

2.44 show reload

	Use this command to display the system restart settings.	
	show reload	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide		
Configuration Examples	The following example displays the restart settings of the system. <pre>FS# show reload Reload scheduled in 595 seconds. At 2003-12-29 11:37:42 Reload reason: test.</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.45 show running-config

	Use this command to display how the current device system is configured..	
	show running-config	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	N/A	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.46 show service

	Use this command to display the service status.	
	show service	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays whether the service is enabled or disabled. <pre>FS# show service web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : enabled telnet-server : disabled</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

2.47 show sessions

	Use this command to display the Telnet Client session information.	
	show sessions	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide	Telnet Client session information includes the VTY number and the server IP address.	
Configuration Examples	The following example displays the Telnet Client session information. <pre>FS#show sessions Conn Address *1 127.0.0.1 *2 192.168.21.122</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.48 show startup-config

	Use this command to display the device configuration stored in the Non Volatile Random Access Memory (NVRAM).	
	show startup-config	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode	

Mode		
Usage Guide	The device configuration stored in the NVRAM is executed while the device is starting. On a device that does not support startup-config is contained in the default configuration file /config.text in the built-in flash memory.	
Configuration Examples	N/A	
Related Commands	Command	Description
	boot config	Sets the name of the boot configuration file.
Platform Description	N/A	

2.49 show this

	Use this command to display effective configuration in the current mode.	
	show this	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	All modes.	
Usage Guide	The configuration in the following range modes cannot be displayed. If the show this command is run, the outcome is NULL. 1. Use the line <i>first-line last-line</i> command to configure lines in a continuous group and enter LINE configuration mode. 2. Use the vlan range command to configure VLANs and enter vlan range configuration mode. Use the interface range command to configure interfaces and enter interface range configuration mode.	
Configuration Examples	The following example displays configuration on interface fastEthernet 0/1. <pre>FS (config)#interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)#show this Building configuration... ! spanning-tree link-type point-to-point spanning-tree mst 0 port-priority 0</pre>	

	<pre> ! end FS (config-if-FastEthernet 0/1)# The following example displays configuration on interface range vlan 1-3. FS(config-if-range)#show this Building configuration... ! interface VLAN 1 ip address dhcp interface VLAN 2 ip address 1.1.1.1 255.255.255.0 interface VLAN 3 ip address 3.3.3.3 255.255.255.0 ! End FS(config-if-range)# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.50 speed

	Use this command to set the speed at which the terminal transmits packets. Use the no form of this command to restore the default setting.	
	speed <i>speed</i>	
	no speed	
Parameter Description	Parameter	Description
	<i>speed</i>	Transmission rate (bps) on the terminal. For serial ports, optional rates include 9600, 19200, 38400, 57600, and 115200 bps. The default rate is 9600 bps.
Defaults	The default is 9600.	
Command Mode	Line configuration mode	
Usage Guide	This command is used to set the speed at which the terminal transmits packets.	

Configuration Examples	The following example sets the rate of the serial port to 57600 bps. <pre>FS(config)# line console 0 FS(config-line)# speed 57600</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.51 telnet

	Use this command to log in a server that supports telnet connection.	
	telnet [oob] <i>host</i> [<i>port</i>] [/ source { ip <i>A.B.C.D</i> ipv6 <i>X:X:X:X::X</i> interface <i>interface-name</i> }]	
Parameter Description	Parameter	Description
	host	The IP address of the host or host name you want to log in.
	Port	Selects the TCP port number for login, 23 by default.
	/source	Specifies the source IP address or source interface used by the Telnet client.
	ip <i>A.B.C.D</i>	Specifies the source IPv4 address used by the Telnet client.
	ipv6 <i>X:X:X:X::X</i>	Specifies the source IPv6 address used by the Telnet client.
	interface <i>interface-name</i>	Specifies the source interface used by the Telnet client.
	oob	Connects to Telnet server through oob channel. This parameter is available only when the device has a MGMT port.
Defaults	N/A	
Command Mode	User EXEC mode	
Usage Guide		
Configuration Examples	The following example sets telnet to IPv4 address 192.168.1.11. The port number is the default, and the source interface is Gi 0/1. The queried VRF routing table is vpn1. <pre>FS# telnet 192.168.1.11 /source-interface gigabitEthernet 0/1 /vrf vpn1</pre> The following example sets telnet to IPv6 address 2AAA:BBBB::CCCC. <pre>FS# telnet 2AAA:BBBB::CCCC</pre>	
Related Commands	Command	Description
	ip telnet source-interface	Specifies the IP address of the interface as the source address for Telnet connection.

	show sessions	Displays the currently established Telnet sessions.
	exit	Exits current connection.
Platform Description	N/A	

2.52 username

	Use this command to set a local username and optional authorization information.. Use the no form of this command to restore the default setting.	
	username <i>name</i> [login mode { aux console ssh telnet }] [online amount <i>number</i>] [permission <i>oper-mode path</i>] [privilege <i>privilege-level</i>] [reject remote-login] [web-auth] [pwd-modify] [nopassword password [0 7] <i>text-string</i>] [secret [0 5] <i>text-string</i>]	
	no username <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Username
	login mode	Sets the login mode.
	aux	Sets the login mode to aux.
	console	Sets the login mode to console.
	ssh	Sets the login mode to ssh.
	telnet	Sets the login mode to telnet.
	online amount <i>number</i>	Sets the amount of users online simultaneously.
	permission <i>oper-mode path</i>	Sets the permission on the specified file. <i>op-mode</i> refers to the operation mode and <i>path</i> to the file or the directory path.
	privilege <i>privilege-level</i>	Sets the privilege level, in the range from 0 to 15.
	reject remote-login	Confines the account to remote login.
	web-auth	Confines the account to web authentication.
	pwd-modify	Allows the web authentication user of this account to change the password. It works only when the web-auth command is configured.
	nopassword	The account is not configured with a password.
	password [0 7] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 7, the password is encrypted. The password is in plain text by default.
	secret [0 5] <i>text-string</i>	If the password type is 0, the password is in plain text. If the type is 5, the password is encrypted. The password is in plain text by default.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to establish a local user database for authentication.	

	 If encryption type is 7, the cipher text you enter should contain seven characters to be valid. In general, do not set the encryption type 7. Instead, specify the type of encryption as 7 only when the encrypted password is copied and pasted.	
Configuration Examples	The following example configures a username and password and binds the user to level 15. <pre>FS(config)# username test privilege 15 password 0 pw15</pre> The following example configures the username and password exclusive to web authentication. <pre>FS(config)# username user1 web-auth password 0 pw</pre> The following example configures user test with read and write permissions on all files and directories. <pre>FS(config)# username test permission rw /</pre> The following example configures user test with read, write and execute permissions on all files and directories except the config.text file. <pre>FS(config)# username test permission n /config.text</pre> <pre>FS(config)# username test permission rwx /</pre>	
Related Commands	Command	Description
	login local	Enables local authentication
Platform Description	N/A	

2.53 username export

	Use this command to export user information to the file.	
	username export <i>filename</i>	
Parameter Description	Parameter	Description
	<i>filename</i>	The file name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to export user information to the file.	
Configuration Examples	The following example exports user information to the file. <pre>FS# username export user.csv</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.54 username import

	Use this command to import user information from the file.	
	username import <i>filename</i>	
Parameter Description	Parameter	Description
	<i>filename</i>	The file name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to import user information from the file.	
Configuration Examples	The following example imports user information from the file.	
	FS# username import user.csv	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.55 write

	Use this command to save running-config at a specified location.	
	write [memory terminal]	
Parameter Description	Parameter	Description
	memory	Writes the system configuration (running-config) into NVRAM, which is equivalent to copy running-config startup-config .
	terminal	Displays the system configuration, which is equivalent to show running-config .

Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Despite the presence of alternative commands, these commands are widely used and accepted. Therefore, they are reserved to facilitate user operations. The system automatically creates the specified file and writes it into system configuration if the device that stores the file exists; The system will ask you whether to save the current configuration in default boot configuration file /config.text and perform an action as required if the device that stores the file does not exist possibly because the boot configuration file is stored on a removable storage device such as USB or SD disk, and the device has not been loaded when you run the write [memory] command.	
Configuration Examples	The following example saves running-config at a specified location. <pre>FS# write Building configuration... [OK]</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3 Line Commands

3.1 access-class

	Use this command to control login into the terminal through IPv4 ACL. Use the no form of this command to restore the default setting.	
	access-class { <i>access-list-number</i> <i>access-list-name</i> } { in out }	
	no access-class { <i>access-list-number</i> <i>access-list-name</i> } { in out }	
Parameter Description	Parameter	Description
	<i>access-list-number</i>	Specifies the ACL number. Standard IP ACL number is from 1 to 99 and from 1300 to 1999. Extended IP ACL number is from 100 to 199 and from 2000 to 2699.
	<i>access-list-name</i>	Specifies the ACL name.
	in	Filters the incoming connections.
	out	Filters the outgoing connections.
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example uses ACL 20 to filter the incoming connections in line VTY 0 5. <pre>FS(config)# line vty 0 5 FS(config-line)access-list 20 in</pre> The following example uses the ACL named "test" to filter the outgoing connections in line VTY 6 7. <pre>FS(config)# line vty 6 7 FS(config-line)access-list test out</pre>	
Related Commands	Command	Description
	show running	Displays status information
Platform Description	N/A	

3.2 accounting commands

	Use this command to enable command accounting in the line. Use the no form of this command to restore the

	default setting.	
	accounting commands <i>level</i> { default <i>list-name</i> }	
	no accounting commands <i>level</i>	
Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
	default	Default authorization list name.
	<i>list-name</i>	Optional list name.
Defaults	This function is disabled by default.	
Command Mode	Line configuration mode	
Usage Guide	This function is used together with AAA authorization. Configure AAA command accounting first, and then apply it on the line.	
Configuration Examples	The following example enables command accounting in line VTY 1 and sets the command level to 15. <pre> FS(config)# aaa new-model FS(config)# aaa accounting commands 15 default start-stop group tacacs+ FS(config)# line vty 1 FS(config-line)# accounting commands 15 default </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.3 accounting exec

	Use this command to enable user access accounting in the line. Use the no form of this command to restore the default setting.	
	accounting commands <i>level</i> { default <i>list-name</i> }	
	no accounting commands <i>level</i>	
Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is accounted when it is executed.
	default	Default authorization list name.

	<i>list-name</i>	Optional list name.
Defaults	This function is disabled by default.	
Command Mode	Line configuration mode	
Usage Guide	This function is used together with AAA authorization. Configure AAA EXEC accounting first, and then apply it on the line.	
Configuration Examples	The following example enables user access accounting in line VTY 1. <pre>FS(config)# aaa new-model FS(config)# aaa accounting exec default start-stop group radius FS(config)# line vty 1 FS(config-line)# accounting exec default</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.4 authorization commands

	Use this command to enable authorization on commands, Use the no form of this command to restore the default setting.	
	authorization commands <i>level</i> { default <i>list-name</i> }	
	no authorization commands <i>level</i>	
Parameter Description	Parameter	Description
	<i>level</i>	Command level ranging from 0 to 15. The command of this level is executed after authorization is performed.
	default	Default authorization list name,
	<i>list-name</i>	Optional list name.
Defaults	This function is disabled by default.	
Command Mode	Line configuration mode	
Usage Guide	This function is used together with AAA authorization. Configure AAA authorization first, and then apply it on the line.	

Configuration	The following example enables authorization on commands of level 15 in line VTY 1.	
Examples	<pre>FS(config)# aaa new-model FS(config)# aaa authorization commands 15 default group tacacs+ FS(config)# line vty 1 FS(config-line)# authorization commands 15 default</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.5 authorization exec

	Use this command to enable EXEC authorization for the line. Use the no form of this command to restore the default setting.	
	authorization { default list-name }	
	no authorization exec	
Parameter Description	Parameter	Description
	default	Default authorization list name,
	<i>list-name</i>	Optional list name.
Defaults	This function is disabled by default,	
Command Mode	Line configuration mode	
Usage Guide	This function is used together with AAA authorization. Configure AAA EXEC authorization first, and then apply it on the line.	
Configuration Examples	The following example performs EXEC authorization to line VTY 1. <pre>FS(config)# aaa new-model FS(config)# aaa authorization exec default group radius FS(config)# line vty 1 FS(config-line)# authorization exec default</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

3.6 clear line

	Use this command to clear connection status of the line.	
	clear line { console <i>line-num</i> vtty <i>line-num</i> <i>line-num</i> }	
Parameter Description	Parameter	Description
	console	Clears connection status of the console line.
	vtty	Clears connection status of the virtual terminal line.
	<i>line-num</i>	Specifies the line to be cleared.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear connection status of the line and restore the line to the unoccupied status to create new connections.	
Configuration Examples	The following example clears connection status of line VTY 13. The connected session on the client (such as Telnet and SSH) in the line is disconnected immediately.	
	FS# clear line vty 13	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.7 disconnect-character

	Use this command to set the hot key that disconnects the terminal service connection. Use the no form of this command to restore the default setting.	
	disconnect-character <i>ascii-value</i>	
	no disconnect-character	
Parameter Description	Parameter	Description
	<i>ascii-value</i>	ASCII decimal value of the hot key that disconnects the terminal service connection, in the range from 0 to 255.

Defaults	The default hot key is Ctrl+D and the ASCII decimal value is 0x04.	
Command Mode	Line configuration mode	
Usage Guide	This command is used to set the hot key that disconnects the terminal service connection. The hot key cannot be the commonly used ASCII node such as characters ranging from a to z, from A to Z or numbers ranging from 0 to 9. Otherwise, the terminal service cannot operate properly.	
Configuration Examples	The following example sets the hot key that disconnects the terminal service connection on line VTY 0 5 to Ctrl+E (0x05). <pre>FS(config)# line vty 0 5 FS(config-line)# disconnect-character 5</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 escape-character

	Use this command to set the escape character for the line. Use the no form of this command to restore the default setting.	
	escape-character <i>escape-value</i>	
	no escape-character	
Parameter Description	Parameter	Description
	<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the line, in the range from 0 to 255.
Defaults	The default escape character is Ctrl+^ (Ctrl+Shift+6) and the ASCII decimal value is 30.	
Command Mode	Line configuration mode	
Usage Guide	After configuring this command, press the key combination of the escape character and then press x , the current session is disconnected to return to the original session.	
Configuration Examples	The following example sets the escape character for the line to 23 (Ctrl+w). <pre>FS(config)# line vty 0</pre>	

	FS(config-line)# escape-character 23	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.9 exec

	Use this command to enable the line to enter the command line interface. Use the no form of this command to disable the function.																													
	exec																													
	no exec																													
Parameter Description	Parameter		Description																											
	N/A		N/A																											
Defaults	This function is enabled by default.																													
Command Mode	Line configuration mode																													
Usage Guide	The no exec command is used to ban the line from entering the command line interface. You have to enter the command line interface through other lines,																													
Configuration Examples	The following example bans line VTY 1 from entering the command line interface. FS(config)# line vty 1 FS(config-line)# no exec FS# show users <table><thead><tr><th>Line</th><th>User</th><th>Host(s)</th><th>Idle</th><th>Location</th></tr></thead><tbody><tr><td colspan="5">-----</td></tr><tr><td>* 0 con 0</td><td>---</td><td>idle</td><td>00:00:00</td><td>---</td></tr><tr><td>1 vty 0</td><td>---</td><td>idle</td><td>00:01:03</td><td>20.1.1.2</td></tr><tr><td>3 vty 2</td><td>---</td><td>idle</td><td>00:00:13</td><td>20.1.1.2</td></tr></tbody></table>					Line	User	Host(s)	Idle	Location	-----					* 0 con 0	---	idle	00:00:00	---	1 vty 0	---	idle	00:01:03	20.1.1.2	3 vty 2	---	idle	00:00:13	20.1.1.2
Line	User	Host(s)	Idle	Location																										

* 0 con 0	---	idle	00:00:00	---																										
1 vty 0	---	idle	00:01:03	20.1.1.2																										
3 vty 2	---	idle	00:00:13	20.1.1.2																										
Related Commands	Command			Description																										
	N/A			N/A																										
Platform Description	N/A																													

3.10 history

	Use this command to enable command history for the line or set the number of commands in the command history. Use the no history command to disable command history. Use the no history size command to restore the number of commands in the command history to the default setting.	
	history [size <i>size</i>]	
	no history	
	no history size	
Parameter Description	Parameter	Description
	size <i>size</i>	The number of commands, in the range from 0 to 256.
Defaults	This function is enabled by default, The default <i>size</i> is 10.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the number of commands in the command history to 20 for line VTY 0 5. <pre>FS(config)# line vty 0 5 FS(config-line)# history size 20</pre> The following example disables the command history for line VTY 0 5. <pre>FS(config)# line vty 0 5 FS(config-line)# no history</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.11 ipv6 access-class

	Use this command to configure access to the terminal through IPv6 ACL. Use the no form of this command to restore the default setting.	
	ipv6 access-class <i>access-list-name</i> { in out }	
	no ipv6 access-class <i>access-list-name</i> { in out }	
Parameter Description	Parameter	Description
	<i>access-list-name</i>	Specifies the ACL name.

	in	Filters the incoming connections.
	out	Filters the outgoing connections.
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example uses the ACL named "test" to filter the outgoing IPv6 connections in line VTY 0 4. <pre>FS(config)# line vty 0 4 FS(config-line)ipv6 access-list test out</pre>	
Related Commands	Command	Description
	show running	Displays status information
Platform Description	N/A	

3.12 length

	Use this command to set the screen length for the line. Use the no form of this command to restore the default setting.	
	length <i>screen-length</i>	
	no length	
Parameter Description	Parameter	Description
	<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.
Defaults	The default is 24.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the screen length to 10. <pre>FS(config-line)# length 10</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.13 line

	Use this command to enter the specified LINE mode.	
	line [console vty] <i>first-line</i> [<i>last-line</i>]	
Parameter Description	Parameter	Description
	console	Console port
	vty	Virtual terminal line, applicable for telnet/ssh connection.
	<i>first-line</i>	Number of first-line to enter
	<i>last-line</i>	Number of last-line to enter
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide		
Configuration Examples	The following example enters the LINE mode from LINE VTY 1 to 3: <pre>FS(config)# line vty 1 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.14 line vty

	Use this command to increase the number of VTY connections currently available. Use the no form of this command to restore the default setting.
	line vty <i>line-number</i>
	no line vty <i>line-number</i>

Parameter Description	Parameter	Description
	<i>line-number</i>	Number of VTY connections, in the range from 0 to 35.
Defaults		
Command Mode	Global configuration mode.	
Usage Guide		
Configuration Examples	The following example increases the number of available VTY connections to 20. The available VTY connections are numbered 0 to 19. <pre>FS(config)# line vty 19</pre> The following example decreases the number of available VTY connections to 10. The available VTY connections are numbered 0-9. <pre>FS(config)# line vty 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.15 location

	Use this command to configure the line location description. Use the no form of this command to restore the default setting.	
	location <i>location</i>	
	no location	
Parameter Description	Parameter	Description
	<i>location</i>	Line location description
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration	The following example describes the line location as Switch's Line VTY 0.	

Examples	FS(config)# line vty 0	
	FS(config-line)# location Switch's Line Vty 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.16 monitor

	Use this command to enable log display on the terminal. Use the no form of this command to restore the default setting,	
	monitor	
	no monitor	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables log display on the terminal in VTY line 0 5.	
	FS(config)# line vty 0 5 FS(config-line)# monitor	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.17 privilege level

	Use this command to set the privilege level for the line. Use the no form of this command to restore the default setting.
	privilege level <i>level</i>

	no privilege level	
Parameter Description	Parameter	Description
	<i>level</i>	Privilege level, in the range from 0 to 15.
Defaults	The default is 1.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the privilege level for the line VTY 0 4 to 14. <pre>FS(config)# line vty 0 4 FS(config-line)privilege level 14</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.18 refuse-message

	Use this command to set the login refusal message for the line. Use the no form of this command to restore the default setting.	
	refuse-message [<i>c message c</i>]	
	no refuse-message	
Parameter Description	Parameter	Description
	<i>c</i>	Delimiter of the login refusal message, which is not allowed within the message.
	<i>message</i>	Login refusal message.
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	This command is used to set the login refusal message for the line. The characters entered after the ending delimiter are discarded directly, The login refusal message is displayed when the user has been refused to login.	

Configuration Examples	The following example sets the login refusal message for the line to "Unauthorized user cannot login to the FS device". FS(config-line)#vacant-message @ Unauthorized user cannot login to the FS device @	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.19 show history

	Use this command to display the command history of the line.	
	show history	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the command history of the line. FS# show history exec: sh privilege sh run show user sh user all show history	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.20 show line

	Use this command to display line configuration.																					
	show line { console <i>line-num</i> vty <i>line-num</i> <i>line-num</i> }																					
Parameter Description	Parameter	Description																				
	console	Displays configuration for the console line.																				
	vty	Displays configuration for the virtual terminal line.																				
	<i>line-num</i>	Displays the line.																				
Defaults	N/A																					
Command Mode	Privileged EXEC mode																					
Usage Guide	N/A																					
Configuration Examples	The following example displays configuration for the console port. <pre>FS# show line console 0 CON Type speed Overruns * 0 CON 9600 45927 Line 0, Location: "", Type: "vt100" Length: 24 lines, Width: 79 columns Special Chars: Escape Disconnect Activation ^^x none ^M Timeouts: Idle EXEC Idle Session never never History is enabled, history size is 10. Total input: 53564 bytes Total output: 395756 bytes Data overflow: 27697 bytes stop rx interrupt: 0 times</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>CON</td><td>Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.</td></tr><tr><td>Type</td><td>Terminal type, including CON, AUX, TTY, and VTY.</td></tr><tr><td>speed</td><td>Asynchronous speed.</td></tr><tr><td>Overruns</td><td>The number of overrun errors received by the flash.</td></tr><tr><td>Line 0</td><td>Terminal line number.</td></tr><tr><td>Location: ""</td><td>Line location configuration.</td></tr><tr><td>Type: "vt100"</td><td>Compatibility standard.</td></tr><tr><td>Special Chars</td><td>Special characters, including Escape, Disconnect, and Activation characters.</td></tr><tr><td>Timeouts</td><td>Timeout value; "never" indicates no timeout.</td></tr></table>		Field	Description	CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.	Type	Terminal type, including CON, AUX, TTY, and VTY.	speed	Asynchronous speed.	Overruns	The number of overrun errors received by the flash.	Line 0	Terminal line number.	Location: ""	Line location configuration.	Type: "vt100"	Compatibility standard.	Special Chars	Special characters, including Escape, Disconnect, and Activation characters.	Timeouts	Timeout value; "never" indicates no timeout.
Field	Description																					
CON	Terminal type. CON indicates console; 0 indicates terminal line number and * ahead of the number means that the terminal is in use.																					
Type	Terminal type, including CON, AUX, TTY, and VTY.																					
speed	Asynchronous speed.																					
Overruns	The number of overrun errors received by the flash.																					
Line 0	Terminal line number.																					
Location: ""	Line location configuration.																					
Type: "vt100"	Compatibility standard.																					
Special Chars	Special characters, including Escape, Disconnect, and Activation characters.																					
Timeouts	Timeout value; "never" indicates no timeout.																					

	History	Whether to enable command history; the number of commands in the command history.
	Total input	Data volume received from the drive.
	Total output	Date volume sent to the drive.
	Data overflow	Overflowing data volume.
	stop rx interrupt	Data reception interruption times.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.21 show privilege

	Use this command to display the privilege level of the line.	
	show privilege	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the privilege level of the line. FS# show privilege Current privilege level is 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.22 show users

	Use this command to display the login user information.																																																																
	show users [all]																																																																
Parameter Description	Parameter	Description																																																															
	all	Displays line user information, including users logging into the line and users not logging into the line.																																																															
Defaults	N/A																																																																
Command Mode	Privileged EXEC mode																																																																
Usage Guide	N/A																																																																
Configuration Examples	The following example displays the information about users logging into the line, <pre>FS# show users</pre> <table><thead><tr><th>Line</th><th>User</th><th>Host(s)</th><th>Idle</th><th>Location</th></tr></thead><tbody><tr><td>0 con 0</td><td>---</td><td>idle</td><td>00:00:46</td><td>---</td></tr><tr><td>1 vty 0</td><td>---</td><td>idle</td><td>00:00:29</td><td>20.1.1.2</td></tr><tr><td>* 2 vty 1</td><td>---</td><td>idle</td><td>00:00:00</td><td>20.1.1.2</td></tr></tbody></table> The following example displays all line user information, <pre>FS(config)# show users all</pre> <table><thead><tr><th>Line</th><th>User</th><th>Host(s)</th><th>Idle</th><th>Location</th></tr></thead><tbody><tr><td>0 con 0</td><td>---</td><td>idle</td><td>00:00:49</td><td>---</td></tr><tr><td>1 vty 0</td><td>---</td><td>idle</td><td>00:00:32</td><td>20.1.1.2</td></tr><tr><td>* 2 vty 1</td><td>---</td><td>idle</td><td>00:00:00</td><td>20.1.1.2</td></tr><tr><td>3 vty 2</td><td>---</td><td></td><td>00:00:00</td><td>---</td></tr><tr><td>4 vty 3</td><td>---</td><td></td><td>00:00:00</td><td>---</td></tr><tr><td>5 vty 4</td><td>---</td><td></td><td>00:00:00</td><td>---</td></tr><tr><td>6 vty 5</td><td>---</td><td></td><td>00:00:00</td><td>---</td></tr></tbody></table>					Line	User	Host(s)	Idle	Location	0 con 0	---	idle	00:00:46	---	1 vty 0	---	idle	00:00:29	20.1.1.2	* 2 vty 1	---	idle	00:00:00	20.1.1.2	Line	User	Host(s)	Idle	Location	0 con 0	---	idle	00:00:49	---	1 vty 0	---	idle	00:00:32	20.1.1.2	* 2 vty 1	---	idle	00:00:00	20.1.1.2	3 vty 2	---		00:00:00	---	4 vty 3	---		00:00:00	---	5 vty 4	---		00:00:00	---	6 vty 5	---		00:00:00	---
Line	User	Host(s)	Idle	Location																																																													
0 con 0	---	idle	00:00:46	---																																																													
1 vty 0	---	idle	00:00:29	20.1.1.2																																																													
* 2 vty 1	---	idle	00:00:00	20.1.1.2																																																													
Line	User	Host(s)	Idle	Location																																																													
0 con 0	---	idle	00:00:49	---																																																													
1 vty 0	---	idle	00:00:32	20.1.1.2																																																													
* 2 vty 1	---	idle	00:00:00	20.1.1.2																																																													
3 vty 2	---		00:00:00	---																																																													
4 vty 3	---		00:00:00	---																																																													
5 vty 4	---		00:00:00	---																																																													
6 vty 5	---		00:00:00	---																																																													
Related Commands	Command			Description																																																													
	N/A			N/A																																																													
Platform Description	N/A																																																																

3.23 speed

	Use this command to configure the baud rate for the specified line. Use the no form of this command to restore the default setting,	
	speed <i>baudrate</i>	
	no speed	
Parameter Description	Parameter	Description
	<i>baudrate</i>	Sets the baud rate, in the range from 9600 to 115200.
Defaults	The default is 9600.	
Command Mode	LINE configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the baud rate to 115200, <pre>FS(config-line)# speed 115200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.24 terminal escape-character

	Use this command to set the escape character for the current terminal. Use the no form of this command to restore the default setting.	
	terminal escape-character <i>escape-value</i>	
	terminal no escape-character	
Parameter Description	Parameter	Description
	<i>escape-value</i>	Sets the ASCII value corresponding to the escape character for the current terminal, in the range from 0 to 255.
Defaults	The default escape character is Ctrl+^ (Ctrl+Shift+6) and the ASCII decimal value is 30.	
Command Mode	Privileged EXEC mode	

Usage Guide	After configuring this command, press the key combination of the escape character and then press x , the current session is disconnected to return to the original session.	
Configuration Examples	The following example sets the escape character for the current terminal to 23 (Ctrl+w). FS# terminal escape-character 23	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.25 terminal history

	Use this command to enable command history for the current terminal or set the number of commands in the command history. Use the no history command to disable command history. Use the no history size command to restore the number of commands in the command history to the default setting.	
	terminal history [size size]	
	terminal no history	
	terminal no history size	
Parameter Description	Parameter	Description
	size size	Sets the number of commands, in the range from 0 to 256.
Defaults	This function is enabled by default, The default <i>size</i> is 10.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the number of commands in the command history to 20 for the current terminal. FS# terminal history size 20 The following example disables the command history for the current terminal. FS# terminal no history	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.26 terminal length

	Use this command to set the screen length for the current terminal. Use the no form of this command to restore the default setting.	
	terminal length <i>screen-length</i>	
	terminal no length	
Parameter Description	Parameter	Description
	<i>screen-length</i>	Sets the screen length, in the range from 0 to 512.
Defaults	The default is 24.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the screen length for the current terminal to 10. <pre>FS# terminal length 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.27 terminal location

	Use this command to configure location description for the current device. Use the no form of this command to restore the default setting.	
	terminal location <i>location</i>	
	terminal no location	
Parameter Description	Parameter	Description
	<i>location</i>	Configures location description of the current device.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A	
Configuration Examples	The following example configures location description of the current device as "Switich's Line Vty 0". <pre>FS# terminal location Switich's Line Vty 0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.28 terminal speed

	Use this command to configure the baud rate for the current terminal. Use the no form of this command to restore the default setting,	
	terminal speed <i>baudrate</i>	
	terminal no speed	
Parameter Description	Parameter	Description
	<i>baudrate</i>	Sets the baud rate, in the range from 9600 to 115200.
Defaults	The default is 9600.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the baud rate for the current terminal to 115200, <pre>FS# terminal speed 115200</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.29 terminal width

	Use this command to set the screen width for the terminal.
	terminal width <i>screen-width</i>

	terminal no width	
Parameter Description	Parameter	Description
	<i>screen-width</i>	Sets the screen width for the terminal, in the range from 0 to 256.
Defaults	The default is 79.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the screen width for the terminal to 10.	
	FS# terminal width 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.30 timeout login

	Use this command to set the login authentication timeout for the line. Use the no form of this command to restore the default setting.	
	timeout login response <i>seconds</i>	
	no timeout login response	
Parameter Description	Parameter	Description
	response	The time period during which the line waits for the user to enter any message.
	<i>seconds</i>	Timeout value, in the range from 1 to 300 in the unit of seconds.
Defaults	The default is 30.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the login authentication timeout to 300 seconds for line VTY 0 5.	
	FS(config)# line vty 0 5	

	FS(config-line)login timeout response 300	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.31 transport input

	Use this command to set the specified protocol under Line that can be used for communication. Use the no form of this command to restore the default setting.	
	transport input { all ssh telnet none }	
	no transport input { all ssh telnet none }	
Parameter Description	Parameter	Description
	all	Allows all the protocols under Line to be used for communication
	ssh	Allows only the SSH protocol under Line to be used for communication
	telnet	Allows only the Telnet protocol under Line to be used for communication
	none	Allows none of protocols under Line to be used for communication
Defaults	all , ssh and telnet protocols are allowed.	
Command Mode	Line configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example specifies that only the Telnet protocol is allowed to login in line vty 0 4. <pre>FS(config)# line vty 0 5 FS(config-line)transport input ssh</pre>	
Related Commands	Command	Description
	show running	Displays status information
Platform Description	N/A	

3.32 vacant-message

	Use this command to set the logout message. Use the no form of this command to restore the default setting.	
	vacant-message [<i>c message c</i>]	
	no vacant-message	
Parameter Description	Parameter	Description
	<i>c</i>	Delimiter of the logout message, which is not allowed within the message.
	<i>message</i>	Logout message.
Defaults	N/A	
Command Mode	Line configuration mode	
Usage Guide	This command is used to set the logout message for the line. The characters entered after the ending delimiter are discarded directly, The logout message is displayed when the user logs out.	
Configuration Examples	The following example sets the logout message to "Logout from the FS device". FS(config-line)#vacant-message @ Logout from the FS device @	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.33 width

	Use this command to set the screen width for the line. Use the no form of this command to restore the default setting,	
	width <i>screen-width</i>	
	no width	
Parameter Description	Parameter	Description
	<i>screen-width</i>	Sets the screen width for the line, in the range from 0 to 256,
Defaults	The default is 79.	
Command Mode	Line configuration mode	

Usage Guide	N/A	
Configuration Examples	The following example sets the screen width for the line to 10. FS(config-line)# width 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4 File System Commands

4.1 cd

	Use this command to set the present directory for the file system.	
	cd [filesystem:] [directory]	
Parameter	Parameter	Description
Description	filesystem:	The URL of filesystem, followed by a colon (:). The filesystem includes flash: , sata: , usb: , and tmp: .
	directory	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The default directory is the flash root directory.	
Command Mode	Privileged EXEC mode.	
Usage Guide		
Configuration Examples	The following example sets the SATA directory. <pre> FS#pwd flash:/ FS#cd sata: FS#pwd sata:/ </pre>	
Related Commands	Command	Description
	pwd	Displays the present word directory.
Platform Description	N/A.	

4.2 copy

	Use this command to copy a file from the specified source directory to the specified destination directory.	
	copy source-url destination-url	
Parameter	Parameter	Description
Description	source-url	Source file URL, which can be local or remote.
	destination-url	Destination file URL, which can be local or remote.

Defaults	N/A.												
Command Mode	Privileged EXEC mode.												
Usage Guide	when the file to be copied exists on the target URL, the target file system determines the action, such as error report, overwrite, or offering you the choice. The following table lists the URL: <table border="1"> <thead> <tr> <th>Prefix</th><th>Description</th></tr> </thead> <tbody> <tr> <td>running-config</td><td>Running configuration file.</td></tr> <tr> <td>startup-config</td><td>startup configuration file.</td></tr> <tr> <td>flash:</td><td>local FLASH file system.</td></tr> <tr> <td>tftp:</td><td>The URL of TFTP network server, in the format as follows: tftp:[[/location]/directory]/filename</td></tr> <tr> <td>oob_tftp: [via mgmt. { number }]</td><td>The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.</td></tr> </tbody> </table>	Prefix	Description	running-config	Running configuration file.	startup-config	startup configuration file.	flash:	local FLASH file system.	tftp:	The URL of TFTP network server, in the format as follows: tftp:[[/location]/directory]/filename	oob_tftp: [via mgmt. { number }]	The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.
Prefix	Description												
running-config	Running configuration file.												
startup-config	startup configuration file.												
flash:	local FLASH file system.												
tftp:	The URL of TFTP network server, in the format as follows: tftp:[[/location]/directory]/filename												
oob_tftp: [via mgmt. { number }]	The URL of TFTP network server connected with the Out-of-Band port, If there are multiple MGMT ports, you can specify one.												
Configuration Examples	The following example copies the netconfig file from device 192.168.64.2 to the FLASH disk and the netconfile file exists locally. <pre>Do you want to overwrite [/data/netconfig]? [Y/N]:y Press Ctrl+C to quit ! Copy success.</pre>												
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>delete</td><td>Deletes the file.</td></tr> <tr> <td>rename</td><td>Renames the file.</td></tr> <tr> <td>dir</td><td>Displays the file list of the specified directory.</td></tr> </tbody> </table>	Command	Description	delete	Deletes the file.	rename	Renames the file.	dir	Displays the file list of the specified directory.				
Command	Description												
delete	Deletes the file.												
rename	Renames the file.												
dir	Displays the file list of the specified directory.												
Platform Description	N/A												

4.3 delete

	Use this command to delete the files in the present directory.	
	delete [<i>filesystem:</i>] <i>file-url</i> startup-config }	
Parameter Description	Parameter	Description
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash , sata , usb , and tmp .
	<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
	startup-config	The startup file.

Defaults	The default <i>filesystem</i> : is flash: .							
Command Mode	Privileged EXEC mode.							
Usage Guide								
Configuration Examples	The following example deletes the fstab file on the FLASH disk. <pre>FS#pwd flash:/ FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,192 bytes total (13,192,656 bytes free) FS#delete flash:/fstab Do you want to delete [flash:/fstab]? [Y/N]:y Delete success. FS#dir Directory of flash:/ 1 -rw- 4096 Jan 03 2012 12:32:09 rc.d 2 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 2 files, 0 directories 10,489,856 bytes total (13,192,992 bytes free)</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>copy</td><td>Copies the file.</td></tr><tr><td>dir</td><td>Displays the file list of the specified directory.</td></tr></table>	Command	Description	copy	Copies the file.	dir	Displays the file list of the specified directory.	
Command	Description							
copy	Copies the file.							
dir	Displays the file list of the specified directory.							
Platform Description	N/A							

4.4 dir

	Use this command to display the files in the present directory.	
	dir [<i>filesystem</i> :] [<i>directory</i>]	
Parameter Description	Parameter	Description
	<i>filesystem</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative

	path.																		
Defaults	By default, only the information under the present working path is displayed.																		
Command Mode	Privileged EXEC mode.																		
Usage Guide																			
Configuration Examples	The following example displays the file information of the root directory in the FLASH disk. <pre>FS#dir flash:/ Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,192 bytes total (13,192,656 bytes free)</pre> <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>1, 2, 3...</td><td>Index number</td></tr> <tr> <td>-rw-</td><td>Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable </td></tr> <tr> <td>10485760</td><td>File size</td></tr> <tr> <td>rpmdb</td><td>File name</td></tr> <tr> <td>files</td><td>File number</td></tr> <tr> <td>directories</td><td>Directory number</td></tr> <tr> <td>total</td><td>Total size</td></tr> <tr> <td>free</td><td>Available space</td></tr> </table>	Field	Description	1, 2, 3...	Index number	-rw-	Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable	10485760	File size	rpmdb	File name	files	File number	directories	Directory number	total	Total size	free	Available space
Field	Description																		
1, 2, 3...	Index number																		
-rw-	Permissions on a file include: ● d: directory ● r: read ● w: write ● x: executable																		
10485760	File size																		
rpmdb	File name																		
files	File number																		
directories	Directory number																		
total	Total size																		
free	Available space																		
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>pwd</td><td>Displays the present directory.</td></tr> <tr> <td>cd</td><td>Sets the present directory of the file system.</td></tr> </table>	Command	Description	pwd	Displays the present directory.	cd	Sets the present directory of the file system.												
Command	Description																		
pwd	Displays the present directory.																		
cd	Sets the present directory of the file system.																		
Platform Description	N/A.																		

4.5 eject

	Use this command to remove the USB.	
	eject [usb0]	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example removes the USB disk. <pre> FS#eject ? usb0 Eject usb disk 0 FS#eject usb0 FS# </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.6 erase

	Use this command to erase the device or file that doesn't have a file system.	
	erase filesystem	
Parameter	Parameter	Description
Description	<i>filesystem:</i>	Name of the file system, followed by a colon (:). For example, usb0:.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration	The following example erases the USB filesystem.	
Examples	FS#erase usb0: Sure to erase usb0:? [Y/N] y Erasing disk usb0 ... Erase disk usb0 done!	
Related		
Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

4.7 file

	Use this command to display the information about a file.	
	file [<i>filesystem:</i>] <i>file-url</i>	
Parameter Description	Parameter	Description
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<i>file-url</i>	The file name containing the path. A file name starts with “/” is an absolute path. Otherwise, it is a relative path.
Defaults	The default <i>filesystem:</i> is flash: .	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about gcc executable file. FS#file flash:/gcc /usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, stripped	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.8 file prompt

	Use this command to set the prompt mode.	
	file prompt [noisy quiet]	
Parameter	Parameter	Description
Description	noisy	Displays prompt for all operation.
	quiet	Displays prompt rarely.
Defaults	The default mode is noisy.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the prompt mode to noisy. FS#file prompt noisy	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.9 mkdir

	Use this command to create a directory.	
	mkdir [<i>filesystem:</i>] <i>directory</i>	
Parameter	Parameter	Description
Description	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The default <i>filesystem:</i> is flash: . The default <i>directory</i> is the root directory.	
Command Mode	Privileged EXEC mode.	
Usage Guide		

Configuration Examples	The following example creates a directory named newdir:	
	<pre> FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,132 bytes total (13,192,656 bytes free) FS#mkdir newdir Created dir flash:/newdir FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 4 drw- 4096 Jan 03 2012 18:13:37 newdir 3 files, 1 directories 10,494,228 bytes total (13,188,560 bytes free) </pre>	
Related Commands	Command	Description
	rmdir	Deletes the directory.
	pwd	Displays the present directory.
Platform Description	N/A	

4.10 more

	Use this command to display the content of a file.	
	more [<i>/ascii</i> <i>/binary</i>] [<i>filesystem:</i>] <i>file-url</i>	
Parameter Description	Parameter	Description
	<i>/ascii</i>	Displays the file content in the ASCII format.
	<i>/binary</i>	Displays the file content in the
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	<i>file-url</i>	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The file is displayed in its own format by default.	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A				
Configuration Examples	The following example displays the content of the netconfig file under root directory of FLASH disk. <pre> FS#more flash:/netconfig # # The network configuration file. This file is currently only used in # conjunction with the TI-RPC code in the libtirpc library. # # Entries consist of: # # <network_id> <semantics> <flags> <protofamily> <protoname> \ # <device> <nametoaddr_libs> # # The <device> and <nametoaddr_libs> fields are always empty in this # implementation. # udp tpi_clts v inet udp - - tcp tpi_cots_ord v inet tcp - - udp6 tpi_clts v inet6 udp - - tcp6 tpi_cots_ord v inet6 tcp - - rawip tpi_raw - inet - - - local tpi_cots_ord - loopback - - - </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

4.11 pwd

	Use this command to display the working path.	
	pwd	
Parameter	Parameter	Description
Description	N/A.	N/A.
Defaults	N/A.	
Usage Guide		
Configuration	The following example switches from FLASH: to SATA:.	
Examples	FS#pwd flash:/	

	<pre>FS#cd sata:/ FS#pwd sata:/</pre>	
Related Commands	Command	Description
	cd	Changes the file system in the present directory.
Platform Description	N/A.	

4.12 rename

	Use this command to move or rename the specified file.	
	rename <i>src-url dst-url</i>	
Parameter Description	Parameter	Description
	<i>src-url</i>	The source file URL to move.
	<i>dst-url</i>	The URL of the destination file or directory.
Defaults	N/A.	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example renames the fstab file in the root directory on the FLASH disk as new-fstab. <pre>FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,192 bytes total (13,192,656 bytes free) FS#rename flash:/fstab flash:/new-fstab Renamed file flash:/new-fstab FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 new-fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,192 bytes total (13,192,656 bytes free)</pre>	

Related Commands	Command	Description
	delete	Deletes the file.
	copy	Copies the file.
Platform Description	N/A	

4.13 rmdir

	Use this command to delete an empty directory.	
	rmdir [<i>filesystem:</i>] <i>directory</i>	
Parameter Description	Parameter	Description
	<i>filesystem:</i>	The URL of file system, followed by a colon (:). The file system includes flash: , sata: , usb: and tmp: .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The default <i>filesystem:</i> is flash: .	
Command Mode	Privileged EXEC mode.	
Usage Guide		
Configuration Examples	The following example deletes the null test directories. <pre> FS#mkdir newdir FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 4 drw- 4096 Jan 03 2012 18:13:37 newdir 3 files, 1 directories 10,494,228 bytes total (13,188,560 bytes free) FS#rmdir newdir removed dir flash:/newdir FS#dir Directory of flash:/ 1 -rw- 336 Jan 03 2012 18:53:42 fstab 2 -rw- 4096 Jan 03 2012 12:32:09 rc.d 3 -rw- 10485760 Jan 03 2012 18:13:37 rpmdb 3 files, 0 directories 10,490,132 bytes total (13,192,656 bytes free) </pre>	

Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

4.14 show file systems

	Use this command to display the file system information.																																																					
	show file systems																																																					
Parameter	Parameter	Description																																																				
Description	N/A.	N/A.																																																				
Defaults	N/A.																																																					
Command Mode	User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode																																																					
Usage Guide																																																						
Configuration Examples	The following example displays the file system information: FS#show file systems <table><thead><tr><th>Size(KB)</th><th>Free(KB)</th><th>Type</th><th>Flags</th><th>Prefixes</th></tr></thead><tbody><tr><td>NA</td><td>NA</td><td>ram</td><td>rw</td><td>tmp:</td></tr><tr><td>NA</td><td>NA</td><td>network</td><td>rw</td><td>tftp:</td></tr><tr><td>NA</td><td>NA</td><td>network</td><td>rw</td><td>oob_tftp:</td></tr><tr><td>NA</td><td>NA</td><td>xmodem</td><td>rw</td><td>xmodem:</td></tr><tr><td>8192</td><td>2416</td><td>disk</td><td>rw</td><td>flash:</td></tr><tr><td>167772160</td><td>147772160</td><td>disk</td><td>rw</td><td>sata0</td></tr><tr><td>1048576</td><td>548576</td><td>disk</td><td>rw</td><td>usb0:</td></tr></tbody></table> <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Size(KB)</td><td>File system space, in the unit of KB.</td></tr><tr><td>Free(KB)</td><td>Available file system space, in the unit of KB.</td></tr><tr><td>Type</td><td>File system type</td></tr><tr><td>Flags</td><td>Permissions on the file system include: - ro: read-only - wo: write-only - rw: read and write </td></tr><tr><td>Prefixes</td><td>File system prefix</td></tr></tbody></table>		Size(KB)	Free(KB)	Type	Flags	Prefixes	NA	NA	ram	rw	tmp:	NA	NA	network	rw	tftp:	NA	NA	network	rw	oob_tftp:	NA	NA	xmodem	rw	xmodem:	8192	2416	disk	rw	flash:	167772160	147772160	disk	rw	sata0	1048576	548576	disk	rw	usb0:	Field	Description	Size(KB)	File system space, in the unit of KB.	Free(KB)	Available file system space, in the unit of KB.	Type	File system type	Flags	Permissions on the file system include: - ro: read-only - wo: write-only - rw: read and write	Prefixes	File system prefix
Size(KB)	Free(KB)	Type	Flags	Prefixes																																																		
NA	NA	ram	rw	tmp:																																																		
NA	NA	network	rw	tftp:																																																		
NA	NA	network	rw	oob_tftp:																																																		
NA	NA	xmodem	rw	xmodem:																																																		
8192	2416	disk	rw	flash:																																																		
167772160	147772160	disk	rw	sata0																																																		
1048576	548576	disk	rw	usb0:																																																		
Field	Description																																																					
Size(KB)	File system space, in the unit of KB.																																																					
Free(KB)	Available file system space, in the unit of KB.																																																					
Type	File system type																																																					
Flags	Permissions on the file system include: - ro: read-only - wo: write-only - rw: read and write																																																					
Prefixes	File system prefix																																																					
Related Commands	Command	Description																																																				
	N/A.	N/A.																																																				

Platform	N/A.
Description	

4.15 show mount

	Use this command to display the mounted information.															
	show mount															
Parameter	Parameter	Description														
Description	N/A	N/A														
Defaults	N/A															
Command Mode	User EXEC mode/Privileged EXEC mode/Global configuration mode/Interface configuration mode															
Usage Guide	N/A															
Configuration Examples	The following example displays the mounted information. FS#show mount /dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0) proc on /proc type proc (rw,noexec,nosuid,nodev) sysfs on /sys type sysfs (rw,noexec,nosuid,nodev) fusectl on /sys/fs/fuse/connections type fusectl (rw) none on /sys/kernel/debug type debugfs (rw) none on /sys/kernel/security type securityfs (rw) udev on /dev type devtmpfs (rw,mode=0755) devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620) tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755) none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880) none on /run/shm type tmpfs (rw,nosuid,nodev) /dev/sda3 on /hao-share type ext3 (rw,commit=0) binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev) <table><tr><th>Field</th><th>Description</th></tr><tr><td>proc</td><td>Source address of mount.</td></tr><tr><td>on</td><td>-</td></tr><tr><td>/proc</td><td>Destination address of mount.</td></tr><tr><td>type</td><td>-</td></tr><tr><td>proc</td><td>Mount type.</td></tr><tr><td>(rw,noexec,nosuid,nodev)</td><td>Mount property.</td></tr></table>		Field	Description	proc	Source address of mount.	on	-	/proc	Destination address of mount.	type	-	proc	Mount type.	(rw,noexec,nosuid,nodev)	Mount property.
Field	Description															
proc	Source address of mount.															
on	-															
/proc	Destination address of mount.															
type	-															
proc	Mount type.															
(rw,noexec,nosuid,nodev)	Mount property.															
Related Commands	Command	Description														
	N/A	N/A														

Platform	N/A
Description	

4.16 tftp-client source

	Use this command to bind a source IP address or source interface with a TFTP client. Use the no or default form of this command to restore the default setting.	
	tftp-client source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> <i>interface</i> }	
	no tftp-client source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> <i>interface</i> }	
	default tftp-client source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> <i>interface</i> }	
Parameter	Parameter	Description
Description	<i>ip-address</i>	Specifies the IPv4 source address.
	<i>ipv6-address</i>	Specifies the IPv6 source address.
	<i>interface</i>	Specifies the source interface
Defaults	No source interface or IP address is bound with the TFTP client by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example binds source IP address 192.168.23.236 with the TFTP client. <pre>FS(config)# tftp-client source ip 192.168.23.236</pre> The following example binds source IPv6 address 2003:0:0:0::2 with the TFTP client. <pre>FS(config)# tftp-client source ipv6 2003:0:0:0::2</pre> The following example binds source interface gigabitEthernet 0/0 with the TFTP client. <pre>FS(config)# tftp-client source gigabitEthernet 0/0</pre> The following example removes the configuration. <pre>FS(config)# no tftp-client source ip 192.168.23.236</pre> The following example restores the default setting. <pre>FS(config)# default tftp-client source ip 192.168.23.236</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

4.17 tree

	Use this command to display the file tree of the current directory.	
	tree [<i>filesystem</i> :] [<i>directory</i>]	
Parameter	Parameter	Description
Description	<i>filesystem</i> :	The URL of file system, followed by a colon (:). The file system includes flash , usb , and tmp .
	<i>directory</i>	The path name. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The default <i>filesystem</i> : is flash .	
Command Mode	User EXEC mode/Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the file tree of flash:/echo <pre> FS#tree flash:/echo +-- client_module +-- client_userspace +-- echo_cli.c +-- echo_client.c +-- echo_client.h +-- echo_client.o +-- echo_cli.o +-- echo_flag.h +-- echo.h +-- echo.ko +-- echo_server.h +-- exec_set_echo.h +-- exec_show_echo.h +-- Makefile +-- module +-- echo.ko +-- echo.mod.c +-- echo.mod.o +-- echo_module.c +-- echo_module.o +-- echo.o +-- echo_server.c +-- echo_server.o +-- echo_sysfs.c </pre>	

	<pre> +-- echo_sysfs.h +-- echo_sysfs.o +-- Makefile +-- modules.order +-- Module.symvers +-- msg_fd.c +-- msg_fd.o +-- readme +-- server_module +-- server_userspace +-- sys_FSOS.ko +-- user_space +-- echo_server.c +-- echo_server.o +-- Makefile +-- msg_fd.c +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free) </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.18 verify

	Use this command to compute, display and verify Message Digest 5 (MD5).	
	verify [/md5 md5-value] filesystem: [file-url]	
Parameter Description	Parameter	Description
	/md5	Computes and displays MD5.
	md5-value	The file MD5, which is compared with the computed MD5.
	filesystem:	The URL of file system, followed by a colon (:). The file system includes flash: , usb: and tmp: .
	file-url	The file name containing the path. A file name starts with "/" is an absolute path. Otherwise, it is a relative path.
Defaults	The default <i>filesystem</i> : is flash: .	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	

Configuration Examples	The following example computes MD5 of flash:/gcc.	
	<pre>FS#verify flash:/gcc 8b072de7db7affd8b2ef824e7e4d716c</pre>	
	The following example computes MD5 and makes a comparison.	
	<pre>FS#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc %SUCCESS verifying /mnt/flash/gcc = 8b072de7db7affd8b2ef824e7e4d716c FS#verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc %Error verifying flash:/gcc Computed signature = 8b072de7db7affd8b2ef824e7e4d716c Submitted signature = 8b072de7db7affd8b2ef824e7e4d71</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.19 show disk

	Use this command to display USB/Flash information.	
	show disk [usb flash]	
Parameter Description	Parameter	Description
	sata	Displays hardware information.
	usb	Displays USB information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays USB information.	
	<pre>FS#show disk usb Disk /dev/sdb: 8159 MB, 8159477760 bytes 252 heads, 62 sectors/track, 1020 cylinders Units = cylinders of 15624 * 512 = 7999488 bytes The following example displays FLASH information.</pre>	
	<pre>FS#show disk flash Nand flash size: 512MB Nor flash size: 1MB</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5 SYS Commands

5.1 calendar set

	Use this command to set the hardware calendar.	
	calendar set { <i>hour</i> [<i>:minute</i> [<i>:second</i>]] } [<i>month</i> [<i>day</i> [<i>year</i>]]]	
Parameter Description	Parameter	Description
	<i>hour</i> [<i>:minute</i> [<i>:second</i>]]	Sets hardware time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can be reset. The unspecified parameters keep the current system values.
	<i>month</i>	Sets month. The range is from 1 to 12.
	<i>day</i>	Sets date. The range is from 1 to 31.
	<i>year</i>	Sets year. The range is from 1970 to 2069.
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	
Usage Guide	The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value. For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the calendar set 12 5 command to change the current time into "2012-05-29 12:33:44".  The hardware time of the system is used as the UTC time, while the software time of the system refers to the local time of the device.  This command is supported by only VSD0.	
Configuration Examples	The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters. <pre>FS# calendar set 6 06:41:39 UTC Fri, Jul 6, 2012</pre> The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters. <pre>FS# calendar set 6:42 06:42:27 UTC Fri, Jul 6, 2012</pre> The following example changes the current hardware time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters.	

	<pre>FS# calendar set 18 3 2</pre> <pre>18:43:05 UTC Fri, Mar 2, 2012</pre>
	 Because the <i>hour</i> parameter is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter 18 (hour), and then enter 3 (month) and 2 (day).
Check Method	-
Platform Description	-

5.2 clock read-calendar

	Use this command to enable the system to synchronize the software time with the hardware time. clock read-calendar	
Parameter Description	Parameter	Description
	-	-
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	
Usage Guide	This command is supported by only VSD0. After you configure this command, the system will synchronize the software time with the current hardware time according to the time zone and summer time settings of the device.	
Configuration Examples	The following example enables the system to synchronize the software time with the hardware time. <pre>FS# clock read-calendar</pre> Set the system clock from the hardware time.	
Check Method	-	
Platform Description	-	

5.3 clock set

	Use this command to set the system software clock. clock set { <i>hour</i> [<i>:minute</i> [<i>:second</i>]] } [<i>month</i> [<i>day</i> [<i>year</i>]]]

Parameter Description	Parameter	Description
	<code>hour [:minute [:second]]</code>	Sets software time in the format of hour: minute: second. Only the specified parameters (hour, minute, or second) can reset. The unspecified parameters keep the current system values.
	<code>month</code>	Sets month. The range is from 1 to 12.
	<code>day</code>	Sets date. The range is from 1 to 31.
	<code>year</code>	Sets year. The range is from 1970 to 2069.
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	
Usage Guide	1. The time parameter is mandatory. After setting time, set month, day, and year, which can be neglected according to your needs. The parameter that is neglected keeps the current system value.  For example, if the current hardware time is "2012-02-29 09:33:44" and you want to change month and hour and keep values of other parameters, use the clock set 12 5 command to change the current time into "2012-05-29 12:33:44".  This command is supported by only VSD0.	
Configuration Examples	The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 6 o'clock and keeps the values of other parameters. <pre>FS# clock set 6 06:48:13 CST Fri, Mar 2, 2012</pre> The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into 06:42 and keeps the values of other parameters. <pre>FS# clock set 6:42 06:42:31 CST Fri, Mar 2, 2012</pre> The following example changes the current software time of the system (for example, 2012-02-01 18:23:06) into March 2 and keeps the values of other parameters. <pre>FS# clock set 18 3 2 18:42:48 CST Fri, Mar 2, 2012</pre>  Because the <i>hour</i> parameter in this command is mandatory, set it to the current time if you do not need to change its value. As shown in the last example, enter 18 (hour), and then enter 3 (month) and 2 (day).	
Check Method	-	

Platform	-
Description	-

5.4 clock summer-time

	Use this command to set the summer time. clock summer-time <i>zone</i> start <i>start-month</i> [<i>week</i> last] <i>start-date hh:mm</i> end <i>end-month</i> [<i>week</i> last] <i>end-date hh:mm</i> [ahead <i>hours-offset</i> [<i>minutes-offset</i>]]	
	Use this command to disable the summer time. no clock summer-time	
Parameter Description	Parameter	Description
	zone	Summer time name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The summer time name contains 3 to 31 characters.
	start	Indicates the start time of the summer time.
	<i>start-month</i>	Start month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Febr and FebRu.
	<i>week</i>	Start week in the start month. The range is from 1 to 5.
	last	The last week of the specified month.
	<i>start-date</i>	Day in the start week of the start month. Value range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The value is not case sensitive and you are allowed to enter an incomplete word, for example, Web and WeDne.
	hh:mm	Time, in the format of hour : minute.
	end	Indicates the end time of the summer time.
	<i>end-month</i>	End month. Value range: January, February, March, April, May, June, July, August, September, October, November, and December. The value is not case sensitive and you may enter an incomplete word, for example, Febr and FebRu.
	ahead	Indicates how much time for the summer time ahead of the standard time during the effective period of the summer time. By default, the summer time is one hour ahead of the standard time.
	<i>hours-offset</i>	Hours ahead of the standard time. The range is from 0 to 12. You are not allowed to set it to 00:00.
	<i>minutes-offset</i>	Minutes ahead of the standard time. The range is from 0 to 59. If <i>hours-offset</i> has been set to 0, you are not allowed to set <i>minutes-offset</i> to 0.
Defaults	-	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	This command is supported by only VSD0.	

Configuration Examples	Assume that the time zone name of your living place is ABC and the standard time is 8:15 ahead of UTC, namely, GMT+08:15. The summer time period starts from the first Saturday in February to the third Monday in May and the summer time is 01:20 ahead of the standard time. In this case, the summer time is 09:35 ahead of the UTC time, but non-summer time is still 08:15 ahead of the UTC time. <pre> FS(config)# clock timezone ABC 8 15 Set time zone name: ABC (GMT+08:15) FS(config)#show clock 16:39:16 ABC Wed, Feb 29, 2012 FS(config)#show calendar 08:24:35 GMT Wed, Feb 29, 2012 FS(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20 *May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute FS# show clock 18:00:08 TZA Wed, Feb 29, 2012 # If the time is set to non-summer time, the time zone name is restored to ABC. FS#clo set 18 1 1 *Jan 1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan 1, 2012 Set system clock: 18:00:09 ABC Sun, Jan 1, 2012 FS#show clock 18:00:12 ABC Sun, Jan 1, 2012 </pre> If the system uses the default summer time that is one hour ahead of the standard time, ahead and the parameters behind ahead can be neglected. For example, set the summer time to start from 2:00 a.m. of the first Sunday in April to 2:00 a.m. of the last Sunday in October and set the summer time to one hour ahead of the standard time. <pre> FS(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00 *May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead 1 hour Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead 1 hour </pre> The following example disables summer time. <pre> FS(config)#no clock summer-time *Jan 1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time. Set no summer time. </pre>
Check Method	-
Platform Description	-

5.5 clock timezone

	Use this command to set the time zone. clock timezone [<i>name</i> <i>hours-offset</i> [<i>minutes-offset</i>]]	
	Use this command to remove the time zone settings. no clock timezone	
Parameter Description	Parameter	Description
	<i>name</i>	Time zone name. It can only be a letter between A and Z or between a and z, which is not case sensitive. The name contains 3 to 31 characters.
	<i>hours-offset</i>	Hours of time difference. It indicates whether the time is faster or smaller than the hardware UTC time. The range is from -12 to 12. The negative digit indicates that the time is slower than the hardware time, while the positive digit indicates that the time is faster than the hardware time.  If the time is slower than the UTC time, add "-" before <i>hours-offset</i>.
	<i>minutes-offset</i>	Minutes of time difference. The range is from 0 to 59.
Defaults	-	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	This command is supported by only VSD0.	
Configuration Examples	The following example sets the time zone name to CST. The software time is 8 hours faster than the hardware time. <pre>FS(config)# clock timezone CST 8 Set time zone name: CST (GMT+08:00)</pre> FS# show clock 18:00:17 CST Wed, Dec 5, 2012 The following example sets the time zone name TZA. The software time is 06:13 slower than the hardware time. <pre>FS(config)# clock timezone TZA -6 13 Set time zone name: TZA (GMT-06:13)</pre> The following example removes the time zone settings. <pre>FS(config)# no clock timezone Set no clock timezone.</pre>	

Check Method	-
Platform Description	-

5.6 clock update-calendar

	Use this command to enable the system to synchronize the hardware time with the software time. clock update-calendar	
Parameter Description	Parameter	Description
	-	-
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	
Usage Guide	This command is supported by only VSD0. After you configure this command, the system will synchronize the hardware time with the current software time according to the time zone and summer time settings of the device.	
Configuration Examples	The following example enables the system to synchronize the hardware time with the software time. <pre>FS# clock update-calendar</pre> Set the hardware time from the system clock. The following example sets the time zone of the hardware time to GMT+5:10, which indicates that the hardware time is 5:10 slower than the software time. The summer time is not set. <pre>FS# show clock 09:30:21 TSZ Wed, Feb 29, 2012</pre> <pre>FS# clock update-calendar</pre> Set the hardware time from the system clock. <pre>FS#show calendar 04:20:25 UTC Wed, Feb 29, 2012</pre> The following example sets the hardware time. If it is set to GMT+5:10 and the summer time is set to be 1:15 faster from the first Monday in February 1 to the second Sunday in June 1, it indicates that the hardware time is 6:25 slower than the software time during the effective period of the summer time. <pre>FS# show clock 09:30:02 TSZ Wed, Feb 29, 2012</pre>	

	<pre>FS# clock update-calendar Set the hardware time from the system clock. FS#show calendar 03:05:08 UTC Wed, Feb 29, 2012</pre>
Check Method	-
Platform Description	-

5.7 cpu high-watermark set

	Use this command to set the watermark range of the CPU usage of the control core and enable CPU usage monitoring. cpu high-watermark set [[up <i>up-value</i>] [down <i>down-value</i>]]	
	Use this command to disable CPU usage monitoring. no cpu high-watermark set	
	Use this command to restore the default settings. default cpu high-watermark set	
Parameter Description	Parameter	Description
	up <i>up-value</i>	Sets the high watermark of the CPU usage. The range is from 1 to 99.
	down <i>down-value</i>	Sets the low watermark of the CPU usage. The range is from 1 to 99.
Defaults	By default, the range of the CPU usage watermark is from 75% and 85%.	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	This command is supported by only VSD0. You can use this command to set the high watermark of the CPU usage and enable CPU usage monitoring. When detecting that the CPU usage exceeds the fluctuation range of the highest watermark, the system prints prompts.	
Configuration Examples	The following example sets the CPU usage watermark to the default value and enables CPU usage monitoring (if it is disabled). <pre>FS(config)# default cpu high-watermark set Reset default cpu watermark monitor Set system cpu high-watermark up 85%, down 75%</pre> The following example disables CPU usage monitoring. <pre>FS(config)# no cpu high-watermark set Close cpu watermark monitor</pre>	

	The following example enables CPU usage monitoring. Keep the defined watermark value. <pre>FS(config)# cpu high-watermark set Open cpu watermark monitor Set system cpu high-watermark up 85%, down 75%</pre> The following example enables CPU usage monitoring and sets the watermark range to 70%-90%. <pre>FS(config)# cpu high-watermark set up 90 down 70 Open cpu watermark monitor Set system cpu high-watermark up 90%, down 70%</pre>
Check Method	-
Prompt Message	If the high watermark of the CPU usage is allowed to fluctuate from 85% to 91%, the system will print the following warning message when the CPU usage exceeds the upper limit of the high watermark: <pre>*Jan 19 16:23:01: %FS_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high watermark(91%),current cpu usage 100%</pre> When the CPU usage is less than the lower limit of the high watermark, the system will print the following message about warning release: <pre>*Jan 20 07:02:52: %FS_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%</pre>
Platform Description	-

5.8 memory history clear

	Use this command to clear the history of the memory usage. memory history clear [one-fourth half all]	
Parameter Description	Parameter	Description
	one-fourth	Clears one fourth entries.
	half	Clears a half of entries.
	all	Clears all the entries.
Defaults	-	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example clears a half of the history of the memory usage. <pre>FS# show memory history</pre>	

	<pre> Time Thu Jan 1 00:24:45 1970 Used(k) 148516 Maxinum memory users for this period Process Name Holding tcpip.elf 270028 cli-memory 60600 syslogd 36640 Time Thu Jan 1 00:24:41 1970 Used(k) 148492 Maxinum memory users for this period Process Name Holding tcpip.elf 270028 cli-memory 52408 syslogd 36640 Time Thu Jan 1 00:24:41 1970 Used(k) 148444 Maxinum memory users for this period Process Name Holding tcpip.elf 270028 cli-memory 44088 syslogd 36640 FS(config)#memory history clear half 2 out of 5 records in the history table to be cleared... Clear done ! </pre>
Check Method	-
Prompt Message	-
Platform Description	-

5.9 memory low-watermark set

	Use this command to set the low watermark threshold of the memory and enable the memory low watermark detection. memory low-watermark set <i>mem-rate</i>
	Use this command to disable the detection of memory low watermark. no memory low-watermark set

Parameter Description	Parameter	Description
	<i>mem-rate</i>	Memory watermark threshold. The range is from 1% to 100%.
Defaults	By default, the memory watermark threshold is 90%.	
Command Mode	Global configuration mode	
Default Level	-	
Usage Guide	You can use this command to enable the detection of the memory low watermark and set the memory watermark threshold. When the system memory is less than this threshold, the system will print prompts.	
Configuration Examples	The following example sets the low watermark threshold of the memory to 80% and enables detection. <pre>FS(config)#memory low-watermark set 80</pre>	
Check Method	-	
Prompt Message	When the system memory is less than the defined watermark value (such as 500000 KB), the system prints the following message: <pre>FS(config)#<187> Jan 1 00:18:59 syslog: Free Memory has dropped below 500000k</pre>	
Platform Description	-	

5.10 reload

	Use this command to reload the device. reload [at { <i>hour</i> [<i>:minute</i> [<i>:second</i>]] } [<i>month</i> [<i>day</i> [<i>year</i>]]]]	
Parameter Description	Parameter	Description
	<i>hour</i> [<i>:minute</i> [<i>:second</i>]]	Sets the restart time in the format of hour : minute : second. Other neglected parameters keep the current system values.
	<i>month</i>	Sets the month, in the range from 1 to 12.
	<i>day</i>	Sets the day, in the range from 1 to 31.
	<i>year</i>	Sets the year, in the range from 1970 to 2069.
Defaults	-	
Command Mode	Privileged EXEC mode	
Default Level	-	

Usage Guide	-
Configuration Examples	The following example reloads the device. <pre>FS# reload Reload system?(Y/N) Y Sending all processes the TERM signal... [OK] Sending all processes the KILL signal... [OK] Restarting system...</pre>
Check Method	-
Prompt Message	-
Platform Description	-

5.11 show calendar

	Use this command to display the hardware calendar. show calendar	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example displays the hardware calendar. <pre>FS# show calendar 21:57:48 GMT Sun, Feb 28, 2012</pre>	
Prompt Message	-	
Platform Description	-	

5.12 show clock

	Use this command to display the system software clock. show clock

Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode / global configuration mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example displays the software clock when the time zone is disabled. <pre>FS# show clock 18:22:20 UTC Tue, Dec 11, 2012</pre> The following example displays the software clock when the time zone is enabled. <pre>FS# show clock 03:07:49 TSZ Wed, Feb 29, 2012</pre>	
Prompt Message	-	
Platform Description	-	

5.13 show memory

	Use this command to display the system memory. show memory [sorted total history low-watermark <i>process-id</i> <i>process-name</i>]	
Parameter Description	Parameter	Description
	sorted total	Ranked according to the memory usage.
	history	Displays the history of memory usage.
	low-watermark	Displays the memory low watermark threshold of the system.
	<i>process-id</i>	Displays the memory usage of the task specified by <i>process-id</i> .
	<i>process-name</i>	Displays the memory usage of the task specified by <i>process-name</i> .
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	Every time when the show memory history command is used, the number of displayed entries increases by one. Up to 10 entries can be displayed. You can use the memory history clear command to clear history entries.	

Configuration Examples	The following example displays the memory usage of each task and the ranking (based on the total memory usage). FS# show memory sorted System Memory: 508324K total, 481560K used, 26764K free, 348200K available, 50.5% used rate Swap: 128000K total, 128000K free Used detail: 149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others <table><tr><th>PID</th><th>Text(K)</th><th>Rss(K)</th><th>Data(K)</th><th>Stack(K)</th><th>Total(K)</th><th>Process</th></tr><tr><td>807</td><td>1568</td><td>4584</td><td>264728</td><td>84</td><td>270028</td><td>tcpip.elf</td></tr><tr><td>854</td><td>40</td><td>1436</td><td>246076</td><td>84</td><td>248840</td><td>cli-filesystem</td></tr><tr><td>1237</td><td>52</td><td>1492</td><td>123260</td><td>84</td><td>126036</td><td>cli-memory</td></tr><tr><td>803</td><td>56</td><td>1104</td><td>74064</td><td>84</td><td>76920</td><td>ping.elf</td></tr><tr><td>727</td><td>84</td><td>1276</td><td>33812</td><td>84</td><td>36640</td><td>syslogd</td></tr><tr><td>733</td><td>84</td><td>796</td><td>33536</td><td>84</td><td>36364</td><td>syslogd</td></tr><tr><td>776</td><td>224</td><td>1416</td><td>16896</td><td>84</td><td>19800</td><td>lsmdemo</td></tr><tr><td>858</td><td>40</td><td>1324</td><td>16844</td><td>84</td><td>19612</td><td>tty-admin</td></tr><tr><td>769</td><td>40</td><td>3600</td><td>11052</td><td>84</td><td>13812</td><td>skbdemo</td></tr></table> --More-- Description of some keywords in the command: <table><tr><th>Keyword</th><th>Description</th></tr><tr><td>total</td><td>Total system memory</td></tr><tr><td>used</td><td>Used memory</td></tr><tr><td>free</td><td>Remaining memory</td></tr><tr><td>used rate</td><td>Memory usage (percentage)</td></tr><tr><td>Active</td><td>Active page</td></tr><tr><td>inactive</td><td>Inactive page</td></tr><tr><td>mapped</td><td>Mapped memory</td></tr><tr><td>slab</td><td>Memory consumed by Slab</td></tr><tr><td>others</td><td>Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.</td></tr></table> Description of the displayed information on each task: <table><tr><th>Field</th><th>Description</th></tr><tr><td>PID</td><td>Process ID</td></tr><tr><td>Text</td><td>Code segment size</td></tr><tr><td>Rss</td><td>Resident memory size</td></tr><tr><td>Data</td><td>Data segment size</td></tr><tr><td>Stack</td><td>Stack size</td></tr><tr><td>Total</td><td>Total used memory</td></tr><tr><td>Process</td><td>Task name</td></tr></table>	PID	Text(K)	Rss(K)	Data(K)	Stack(K)	Total(K)	Process	807	1568	4584	264728	84	270028	tcpip.elf	854	40	1436	246076	84	248840	cli-filesystem	1237	52	1492	123260	84	126036	cli-memory	803	56	1104	74064	84	76920	ping.elf	727	84	1276	33812	84	36640	syslogd	733	84	796	33536	84	36364	syslogd	776	224	1416	16896	84	19800	lsmdemo	858	40	1324	16844	84	19612	tty-admin	769	40	3600	11052	84	13812	skbdemo	Keyword	Description	total	Total system memory	used	Used memory	free	Remaining memory	used rate	Memory usage (percentage)	Active	Active page	inactive	Inactive page	mapped	Mapped memory	slab	Memory consumed by Slab	others	Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.	Field	Description	PID	Process ID	Text	Code segment size	Rss	Resident memory size	Data	Data segment size	Stack	Stack size	Total	Total used memory	Process	Task name
PID	Text(K)	Rss(K)	Data(K)	Stack(K)	Total(K)	Process																																																																																																					
807	1568	4584	264728	84	270028	tcpip.elf																																																																																																					
854	40	1436	246076	84	248840	cli-filesystem																																																																																																					
1237	52	1492	123260	84	126036	cli-memory																																																																																																					
803	56	1104	74064	84	76920	ping.elf																																																																																																					
727	84	1276	33812	84	36640	syslogd																																																																																																					
733	84	796	33536	84	36364	syslogd																																																																																																					
776	224	1416	16896	84	19800	lsmdemo																																																																																																					
858	40	1324	16844	84	19612	tty-admin																																																																																																					
769	40	3600	11052	84	13812	skbdemo																																																																																																					
Keyword	Description																																																																																																										
total	Total system memory																																																																																																										
used	Used memory																																																																																																										
free	Remaining memory																																																																																																										
used rate	Memory usage (percentage)																																																																																																										
Active	Active page																																																																																																										
inactive	Inactive page																																																																																																										
mapped	Mapped memory																																																																																																										
slab	Memory consumed by Slab																																																																																																										
others	Memory capacity of the used memory except the memory used by active and inactive pages, mapped memory, and slab memory.																																																																																																										
Field	Description																																																																																																										
PID	Process ID																																																																																																										
Text	Code segment size																																																																																																										
Rss	Resident memory size																																																																																																										
Data	Data segment size																																																																																																										
Stack	Stack size																																																																																																										
Total	Total used memory																																																																																																										
Process	Task name																																																																																																										
Prompt Message	-																																																																																																										
Platform Description	-																																																																																																										

5.14 show memory vsd

	Use this command to display memory information. show memory vsd <i>vsd_id</i>																																																																																																																																																																																												
Parameter Description	Parameter			Description																																																																																																																																																																																									
	<i>vsd_id</i>			VSD ID is a digit. You can use the show vsd command to display the ID of each VSD. The ID range is from 0 to 16.																																																																																																																																																																																									
Command Mode	Privileged EXEC mode/ global configuration mode																																																																																																																																																																																												
Default Level	-																																																																																																																																																																																												
Usage Guide	 This command is supported only in VSD0 mode.																																																																																																																																																																																												
Configuration Examples	The following example displays the memory usage of each task in VSD 1 mode. <pre>FS#show memory vsd 1</pre> <table><thead><tr><th>PID</th><th>Text</th><th>Rss</th><th>Data</th><th>Stack</th><th>Total</th><th>Process</th></tr></thead><tbody><tr><td>1408</td><td>244</td><td>1192</td><td>25400</td><td>84</td><td>32164</td><td>tty_secu_enable</td></tr><tr><td>1385</td><td>104</td><td>16288</td><td>648</td><td>84</td><td>18648</td><td>gvpd</td></tr><tr><td>1384</td><td>304</td><td>3872</td><td>17084</td><td>84</td><td>24728</td><td>wbamain</td></tr><tr><td>1382</td><td>376</td><td>17708</td><td>33656</td><td>84</td><td>53308</td><td>snooping.elf</td></tr><tr><td>1381</td><td>84</td><td>2156</td><td>16736</td><td>84</td><td>22956</td><td>password_policy</td></tr><tr><td>1380</td><td>72</td><td>1096</td><td>404</td><td>84</td><td>3848</td><td>dns_client.elf</td></tr><tr><td>1379</td><td>168</td><td>2580</td><td>472</td><td>84</td><td>5352</td><td>rmond</td></tr><tr><td>1378</td><td>652</td><td>3504</td><td>9768</td><td>84</td><td>15964</td><td>snmpd</td></tr><tr><td>1376</td><td>208</td><td>1452</td><td>10672</td><td>84</td><td>14872</td><td>fsui</td></tr><tr><td>1375</td><td>116</td><td>2020</td><td>33464</td><td>84</td><td>37288</td><td>telnetc</td></tr><tr><td>1373</td><td>24</td><td>844</td><td>220</td><td>84</td><td>2824</td><td>telnetd</td></tr><tr><td>1372</td><td>724</td><td>2364</td><td>17016</td><td>84</td><td>24380</td><td>sshd</td></tr><tr><td>1371</td><td>244</td><td>2996</td><td>35780</td><td>84</td><td>42544</td><td>tty-admin</td></tr><tr><td>1365</td><td>132</td><td>2168</td><td>9004</td><td>84</td><td>13796</td><td>vrrp_plus.elf</td></tr><tr><td>1364</td><td>312</td><td>16944</td><td>764</td><td>84</td><td>20368</td><td>vrrp.elf</td></tr><tr><td>1363</td><td>124</td><td>16988</td><td>500</td><td>84</td><td>19744</td><td>lACP.elf</td></tr><tr><td>1358</td><td>24</td><td>1380</td><td>320</td><td>84</td><td>3536</td><td>ftpc_cli.elf</td></tr><tr><td>1357</td><td>124</td><td>1944</td><td>8552</td><td>84</td><td>14976</td><td>ftp_server.elf</td></tr><tr><td>1352</td><td>340</td><td>3032</td><td>74704</td><td>84</td><td>80768</td><td>dhcp6.elf</td></tr><tr><td>1351</td><td>312</td><td>1960</td><td>988</td><td>84</td><td>6116</td><td>dhcp.elf</td></tr><tr><td>1350</td><td>388</td><td>17808</td><td>920</td><td>84</td><td>21600</td><td>mstp.elf</td></tr><tr><td>1349</td><td>240</td><td>3876</td><td>976</td><td>84</td><td>9536</td><td>rpi.elf</td></tr><tr><td>1348</td><td>1316</td><td>4656</td><td>1004</td><td>84</td><td>10764</td><td>isis.elf</td></tr><tr><td>1347</td><td>212</td><td>4220</td><td>872</td><td>84</td><td>9368</td><td>ripng.elf</td></tr><tr><td>1345</td><td>460</td><td>4284</td><td>876</td><td>84</td><td>9656</td><td>rip.elf</td></tr></tbody></table>							PID	Text	Rss	Data	Stack	Total	Process	1408	244	1192	25400	84	32164	tty_secu_enable	1385	104	16288	648	84	18648	gvpd	1384	304	3872	17084	84	24728	wbamain	1382	376	17708	33656	84	53308	snooping.elf	1381	84	2156	16736	84	22956	password_policy	1380	72	1096	404	84	3848	dns_client.elf	1379	168	2580	472	84	5352	rmond	1378	652	3504	9768	84	15964	snmpd	1376	208	1452	10672	84	14872	fsui	1375	116	2020	33464	84	37288	telnetc	1373	24	844	220	84	2824	telnetd	1372	724	2364	17016	84	24380	sshd	1371	244	2996	35780	84	42544	tty-admin	1365	132	2168	9004	84	13796	vrrp_plus.elf	1364	312	16944	764	84	20368	vrrp.elf	1363	124	16988	500	84	19744	lACP.elf	1358	24	1380	320	84	3536	ftpc_cli.elf	1357	124	1944	8552	84	14976	ftp_server.elf	1352	340	3032	74704	84	80768	dhcp6.elf	1351	312	1960	988	84	6116	dhcp.elf	1350	388	17808	920	84	21600	mstp.elf	1349	240	3876	976	84	9536	rpi.elf	1348	1316	4656	1004	84	10764	isis.elf	1347	212	4220	872	84	9368	ripng.elf	1345	460	4284	876	84	9656	rip.elf
PID	Text	Rss	Data	Stack	Total	Process																																																																																																																																																																																							
1408	244	1192	25400	84	32164	tty_secu_enable																																																																																																																																																																																							
1385	104	16288	648	84	18648	gvpd																																																																																																																																																																																							
1384	304	3872	17084	84	24728	wbamain																																																																																																																																																																																							
1382	376	17708	33656	84	53308	snooping.elf																																																																																																																																																																																							
1381	84	2156	16736	84	22956	password_policy																																																																																																																																																																																							
1380	72	1096	404	84	3848	dns_client.elf																																																																																																																																																																																							
1379	168	2580	472	84	5352	rmond																																																																																																																																																																																							
1378	652	3504	9768	84	15964	snmpd																																																																																																																																																																																							
1376	208	1452	10672	84	14872	fsui																																																																																																																																																																																							
1375	116	2020	33464	84	37288	telnetc																																																																																																																																																																																							
1373	24	844	220	84	2824	telnetd																																																																																																																																																																																							
1372	724	2364	17016	84	24380	sshd																																																																																																																																																																																							
1371	244	2996	35780	84	42544	tty-admin																																																																																																																																																																																							
1365	132	2168	9004	84	13796	vrrp_plus.elf																																																																																																																																																																																							
1364	312	16944	764	84	20368	vrrp.elf																																																																																																																																																																																							
1363	124	16988	500	84	19744	lACP.elf																																																																																																																																																																																							
1358	24	1380	320	84	3536	ftpc_cli.elf																																																																																																																																																																																							
1357	124	1944	8552	84	14976	ftp_server.elf																																																																																																																																																																																							
1352	340	3032	74704	84	80768	dhcp6.elf																																																																																																																																																																																							
1351	312	1960	988	84	6116	dhcp.elf																																																																																																																																																																																							
1350	388	17808	920	84	21600	mstp.elf																																																																																																																																																																																							
1349	240	3876	976	84	9536	rpi.elf																																																																																																																																																																																							
1348	1316	4656	1004	84	10764	isis.elf																																																																																																																																																																																							
1347	212	4220	872	84	9368	ripng.elf																																																																																																																																																																																							
1345	460	4284	876	84	9656	rip.elf																																																																																																																																																																																							

	1344 1800 5568 1572 84 12156 bgp.elf 1340 1084 4700 1024 84 10928 ldp.elf 1339 288 17684 556 84 21472 msf.elf 1338 208 3604 42712 84 47708 syslogd --More--
Prompt Message	-
Platform Description	-

5.15 show pci-bus

	Use this command to display the information on the device mounted to the PCI bus. show pci-bus	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example displays the information on the device mounted to the PCI bus. <pre> FS# show pci-bus NO:0 Vendor ID : 0x1131 Device ID : 0x1561 Domain:bus:dev.func : 0000:00:05.0 Status / Command : 0x2100000 Class / Revision : 0xc031030 Latency : 0x0 first 64 bytes of configuration address space: 00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00 10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15 30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a NO:1 Vendor ID : 0x1131 Device ID : 0x1562 Domain:bus:dev.func : 0000:00:05.1 </pre>	

	Status / Command : 0x2100156 Class / Revision : 0xc032030 Latency : 0x30 First 64 bytes of configuration address space: 00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00 10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15 30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
Prompt Message	-
Platform Description	-

5.16 show processes cpu

	Use this command to display system task information. show processes cpu [history [table] [[5sec 1min 5min 15min] [nonzero]]	
Parameter Description	Parameter	Description
	5sec 1min 5min 15min	Displays lists of tasks in descending order of CPU usage within the last five seconds, one minute, five minutes, and 15 minutes.
	nonzero	Does not display the task with 0 CPU usage.
	history	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in histogram.
	table	Displays the CPU usage of the control core within the last 60 seconds, 60 minutes, and 72 hours in table.
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	This command is only supported by VSD0.	
Configuration Examples	The following example displays the tasks listed in ascending order of task IDs. <pre> FS# show processes cpu System Uptime: 19:08.6 CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8% set system cpu watermark (open): high 80%(85%~75%) Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie Pid Vsd S PRI P 5Sec 1Min 5Min 15Min Process 1 0 S 20 0 0.0(0.0) 0.0(0.0) 0.0(0.0) 0.0(0.0) init </pre>	

```

 2  0 S   20  1  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) kthreadd
 3  0 S  -100  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/0
 4  0 S   20  0  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) ksoftirqd/0
 5  0 S  -100  1  0.0(0.0)  0.0(0.0)  0.0(0.0)  0.0(0.0) migration/1

```

--More--

The following example displays the tasks listed in ascending order of task IDs without displaying the tasks with 0 CPU usage within 15 minutes.

```
FS# show processes cpu nonzero
```

Description of the information displayed in this command:

Field	Description
System Uptime	Total running time of the device, precious to seconds.
CPU Utilization	Total CPU usage of the control core within the last five seconds, one minute, and five minutes.
Virtual CPU usage	Total CPU usage of the virtual control core within the last five seconds, one minute, and five minutes.
Tasks Statistics	Task statistics information, including the total number of statistics tasks and the task status.
set system cpu watermark	CPU watermark value and status of the control core.

The task running statuses are listed below:

Task Running Status	Description
running	Running task
sleeping	Suspended task
stopped	Stopped task
zombie	Terminated task, but not reclaimed by the system

Description of each task:

Field	Description
Pid	Task ID
Vsd	VSD ID
S	Task status. Five statuses in total: R (running), T (stopped), S (sleeping), D (waiting), and Z (zombie).
PRI	Task running priority
P	The core of the CPU on which the task runs
5sec/1min/5min/15min	CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs.
Process	Task name. Only the first 15 characters are displayed. The remaining characters are truncated.

The following example displays the CPU usage in ascending order of task IDs and only the processes with non-zero CPU usage within 15 minutes are displayed.

```
FS #show processes cpu nonzero
```

The following example displays the CPU usage in descending order within five seconds and the tasks with zero CPU usage within one second are not displayed.

```
FS #show processes cpu 5sec nonzero
```

The following example displays the CPU usage of the control core in histograms within the last 60 seconds, 60 minutes, and 72 hours.

The first histogram displays the CPU usage of the control core within 300 seconds. Every segment in the x-coordinate is five seconds, and every segment in the y-coordinate is 5%. The symbol "*" indicates the CPU usage at the last specified second. In other words, the first segment on the x-coordinate nearest to 0 is the CPU usage in the last five seconds, measured in %.

The second histogram displays the CPU usage of the control core within the last 60 minutes, measured in %. Every segment on the x-coordinate is 1 minute.

The third histogram displays the CPU usage of the control core within the last 72 hours, measured in %. Every segment on the x-coordinate is 1 hour.

Example:

```
FS#show processes cpu history
```

```

                                system cpu percent usage(%) [last 300 second]
                                —
100|
 95|
 90|
 85|
 80|
 75|
 70|
 65|
 60|
 55|
 50|
 45|
 40|*****
 35||||||||
 30||||||||*
 25||||||||
 20||||||||
 15||||||||
 10||||||||
  5||||||||*****
  0||||||||
    #=====#=====#=====*>

```

```

0      50      100      second
system cpu percent usage(%) per 5second (last 125 second)
-----

system cpu percent usage(%) [last 60 minute]
-
100|
95|
90|
85|
80|
75|
70|
65|
60|
55|
50|
45|
40|
35|
30|*
25||
20||
15||
10||
5||*
0||
#==*==>
0      minute
system cpu percent usage(%) per 1minute (last 2 minute)
-----

```

The following example displays the CPU usage of the core 0 in tables within the last 60 seconds, 60 minutes, and 72 hours.

The first table lists the CPU usage within 300 seconds. The first cell indicates the CPU usage within the last five seconds.

The second table lists the CPU usage within the last 60 minutes, measured in %. The two adjacent cells show the CPU usage measured at an interval of one minute.

The third table lists the CPU usage within the last 72 hours, measured in %. The two adjacent cells show the CPU usage measured at an interval of one hour.

Example:

```

FS #show processes cpu history table
system cpu percent usage(%) [last 300 second]
#-----#

```

	<pre> 1 2 3 4 5 6 7 8 9 10 #-----# #-----# 0 2.0 2.4 2.3 2.3 2.8 3.0 2.7 3.2 2.6 2.4 #-----# 1 2.7 2.5 2.7 2.2 2.4 2.6 2.2 2.7 2.3 2.5 #-----# 2 2.9 2.0 2.4 2.5 2.7 2.4 2.4 2.6 2.6 2.5 #-----# 3 2.7 2.8 2.8 3.2 2.5 3.2 3.1 4.0 2.7 2.7 #-----# 4 4.0 2.3 2.1 2.2 2.7 2.4 2.5 2.6 2.4 2.6 #-----# 5 2.4 3.2 2.5 2.3 2.3 3.6 2.8 2.5 2.2 2.4 #-----# system cpu percent usage(%) [last 60 minute] #-----# 1 2 3 4 5 6 7 8 9 10 #-----# #-----# 0 2.6 2.5 3.0 2.4 2.6 #-----# </pre>
Prompt Message	-
Platform Description	-

5.17 show processes cpu detailed

	Use this command to display the details of the specified task. show processes cpu detailed { <i>process-id</i> <i>process-name</i> }	
Parameter Description	Parameter	Description
	<i>process-id</i>	Displays the information on the task of the specified task ID.
	<i>process-name</i>	Displays the information on the task of the specified task name.
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	This command is only supported by VSD0.	

Configuration	The following example displays the information on the task of the specified task name.																				
Examples	<pre> FS# show processes cpu detailed demo Process Id : 1820 Process Name : demo Vsdid : 0 Process Ppid : 1 State : R(running) On CPU : 0 Priority : 20 Age Time : 24:06.5 Run Time : 00:01.0 Cpu Usage : Last 5 sec 0.3% (0.6%) Last 1 min 0.3% (0.6%) Last 5 min 0.3% (0.6%) Last 15 min 0.3% (0.6%) Tty : ? </pre>																				
	 Code Usage: 209.6 KB. If the specified task name is not unique, the system displays the following message:																				
	<pre> FS# show processes cpu detailed demo duplicate process, choose one by id not name. name: demo, id: 1089, state: S(sleeping) name: demo, id: 1091, state: R(running) process name: monitor_procs, do NOT exist, or NOT only one. </pre> Description of the displayed information:																				
	<table border="1"> <thead> <tr> <th>Field</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Process Id</td><td>Task ID</td></tr> <tr> <td>Vsdid</td><td>VSD ID of the task</td></tr> <tr> <td>Process Name</td><td>Task name</td></tr> <tr> <td>Process Ppid</td><td>Parent process task ID</td></tr> <tr> <td>State</td><td>Task running status</td></tr> <tr> <td>On CPU</td><td>CPU where the task is running</td></tr> <tr> <td>Priority</td><td>Task priority</td></tr> <tr> <td>Age Time</td><td>Duration for the task from self-startup to now</td></tr> <tr> <td>Run Time</td><td>Duration for the task from self-startup to being executed</td></tr> </tbody> </table>	Field	Description	Process Id	Task ID	Vsdid	VSD ID of the task	Process Name	Task name	Process Ppid	Parent process task ID	State	Task running status	On CPU	CPU where the task is running	Priority	Task priority	Age Time	Duration for the task from self-startup to now	Run Time	Duration for the task from self-startup to being executed
Field	Description																				
Process Id	Task ID																				
Vsdid	VSD ID of the task																				
Process Name	Task name																				
Process Ppid	Parent process task ID																				
State	Task running status																				
On CPU	CPU where the task is running																				
Priority	Task priority																				
Age Time	Duration for the task from self-startup to now																				
Run Time	Duration for the task from self-startup to being executed																				

	Cpu Usage CPU usage of the task within the last five seconds, one minute, five minutes, and 15 minutes. The value in the round brackets is the CPU usage that is not divided by the total number of cores where the task runs. For example, the demo task is running on No.0 core, which is the control core and the system has two control cores. In this case, the CPU usage is 0.3% (0.6%). Tty Tty ID, in the format of "Primary device ID, secondary device ID". If it is 0, the value is ?. Code Usage Size occupied by the task code segment
	The following example displays the information on the task of the specified task ID. <pre> FS# show process cpu detailed 1715 Process Id : 130 Process Name : crypto Vsdid : 0 Process Ppid : 2 State : S(sleeping) On CPU : 0 Priority : 0 Age Time : 03:41:09.9 Run Time : 00:00.0 Cpu Usage : Last 5 sec 0.0%(0.0%) Last 1 min 0.0%(0.0%) Last 5 min 0.0%(0.0%) Last 15 min 0.0%(0.0%) Tty : ? Code Usage : 0.0KB. </pre>
Prompt Message	-
Platform Description	-

5.18 show usb-bus

	Use this command to display the information on the device mounted to the USB bus.	
	show usb-bus	
Parameter Description	Parameter	Description
	-	-

Command Mode	Privileged EXEC mode/ global configuration mode
Default Level	-
Usage Guide	-
Configuration Examples	1: The following example displays the information on the device mounted to the USB bus. <pre>FS# show usb-bus Device: Linux Foundation 2.0 root hub Bus 001 Device 001: ID 1d6b:0002</pre>
Prompt Message	-
Platform Description	-

5.19 show version

	Use this command to display the system version information. show version	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	-	
Usage Guide	The following example displays the system version information. <pre>FS# show version System description : FS Indoor AP320-I (802.11a/n and 802.11b/g/n) By FS Networks System start time : 2012-12-06 00:00:00 System uptime : 0:03:20:07 System hardware version : 1.0.0 System software version : AP_FSOS11.0(1B1) System serial number : 1234942570018 System boot version : 1.0.0</pre>	
Prompt Message	-	

Platform Description	-

5.20 show cpu

	Use this command to display the information on the system task running on the control core instead of the non-virtual core. show cpu	
Parameter Description	Parameter	Description
	-	-
Command Mode	Privileged EXEC mode/ global configuration mode	
Default Level	-	
Usage Guide	This command is supported only in VSD0 mode. Multiple VSDs are not supported. If the system is equipped with a virtual core, you can use the show processes cpu command to check the CPU usage of the virtual core.	
Configuration Examples	The following example displays the information on the system task running on the control core instead of the non-virtual core. <pre>FS#show cpu ===== CPU Using Rate Information CPU utilization in five seconds: 4.80% CPU utilization in one minute: 4.10% CPU utilization in five minutes: 4.00% NO 5Sec 1Min 5Min Process 1 0.00% 0.00% 0.00% init 2 0.00% 0.00% 0.00% kthreadd 3 0.00% 0.00% 0.00% ksoftirqd/0 4 0.00% 0.00% 0.00% events/0 --More--</pre>	
Prompt Message	-	
Platform Description	-	

5.21 show reboot-reason

	Use this command to display the reboot reason. show reboot-reason [<i>all</i>]

Parameter Description	Parameter	Description
	<i>all</i>	Displays the reboot reason of all devices/service modules
Command Mode	Privileged EXEC mode/ global configuration mode/ User EXEC mode	
Default Level	-	
Usage Guide	-	
Configuration Examples	The following example displays the reboot reason of the device. <pre>FS#show reboot-reason time: 1970-01-01 08:03:13 reason: reload cmd info: /sbin/sysmon/3844 FS#</pre>	
Prompt Message	-	
Platform Description	-	

6 Time Range Commands

6.1 absolute

	Use this command to configure an absolute time range. absolute { [<i>start time date</i>] [<i>end time date</i>] }	
	Use the no form of this command to remove the absolute time range. no absolute	
Parameter Description	Parameter	Description
	start <i>time date</i>	Indicates the start time of the range.
	end <i>time date</i>	Indicates the end time of the range.
Defaults	The default absolute time range is the maximum range, which is from 00:00 January 1, 0 to 23:59 December 31, 9999.	
Command Mode	Time range configuration mode	
Default Level	14	
Usage Guide	Use the absolute command to configure a time absolute time range between a start time and an end time to allow a certain function to take effect within the absolute time range. The maximum absolute time range is from 00:00 January 1, 0 to 23:59 December 31, 9999.	
Configuration Examples	The following example creates a time range and enters time range configuration mode. <pre>FS(config)# time-range no-http FS(config-time-range)#</pre> The following example configures an absolute time range. <pre>FS(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014</pre>	
Check Method	Use the show time-range [<i>time-range-name</i>] command to display the time range configuration.	
Prompt Message	-	
Platform Description	-	

6.2 periodic

	Use this command to configure periodic time. periodic <i>day-of-the-week</i> time to [<i>day-of-the-week</i>] <i>time</i>	
	Use the no form of this command to remove the configured periodic time. no periodic <i>day-of-the-week</i> time to [<i>day-of-the-week</i>] <i>time</i>	
Parameter Description	Parameter	Description
	<i>day-of-the-week</i>	Indicates the week day when the periodic time starts or ends.
	<i>time</i>	Indicates the exact time when the periodic time starts or ends.
Defaults	No periodic time is configured by default.	
Command Mode	Time range configuration mode	
Default Level	14	
Usage Guide	Use the periodic command to configure a periodic time interval to allow a certain function to take effect within the periodic time. If you want to modify the periodic time, it is recommended to disassociate the time range first and associate the time range after the periodic time is modified.	
Configuration Examples	The following example creates a time range and enters time range configuration mode. <pre>FS(config)# time-range no-http FS(config-time-range)#</pre> The following example configures a periodic time interval. <pre>FS(config-time-range)# periodic Monday 1:1 to Tuesday 2:2</pre>	
Check Method	Use the show time-range [<i>time-range-name</i>] command to display the time range configuration.	
Prompt Message	-	
Platform Description	-	

6.3 show time-range

	Use this command to display the time range configuration. show time-range [<i>time-range-name</i>]

Parameter Description	Parameter	Description
	<i>time-range-name</i>	Displays a specified time range.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	Use this command to check the time range configuration.	
Configuration Examples	The following example displays the time range configuration. <pre>FS# show time-range time-range entry: test (inactive) absolute end 01:02 02 February 2012</pre>	
Prompt Message	-	
Platform Description	-	

6.4 time-range

	Use this command to create a time range and enter time range configuration mode. time-range <i>time-range-name</i>	
	Use the no form of this command to remove the configured time range. no time-range <i>time-range-name</i>	
Parameter Description	Parameter	Description
	<i>time-range-name</i>	Time range name
Defaults	No time range is configured by default.	
Command Mode	Global configuration mode	
Default Level	2	
Usage Guide	Some applications (such as ACL) may run based on time. For example, an ACL can be effective within certain time ranges of a week. To this end, first you must configure a time range. After the time range is created, you can configure	

	relevant time control in time range mode.
Configuration Examples	The following example creates a time range. <pre>FS(config)# time-range no-http FS(config-time-range)#</pre>
Check Method	Use the show time-range [<i>time-range-name</i>] command to display the time range configuration.
Prompt Message	-
Platform Description	-

7 HTTP Service Commands

7.1 enable service web-server

	Use this command to enable the HTTP service function. Use the no form of this command to disable the HTTP service function.	
	enable service web-server [http https all]	
	{ no default } enable service web-server [http https all]	
Parameter Description	Parameter	Description
	http	Enables the HTTP service.
	https	Enables the HTTPS service.
	all	Enables both the HTTP service and the HTTPS service.
Defaults	By default, the HTTP service function is disabled.	
Command mode	Global configuration mode.	
Usage Guide	If run a command ends with the keyword all or without keyword, it indicates enabling both the HTTP service and the HTTPS service; if run a command ends with keyword http , it indicates enabling the HTTP service; if run a command ends with keyword https , it indicates enabling the HTTPS service. Use the command no enable service web-server to disable the corresponding HTTP service.	
Configuration Examples	The following example enables both the HTTP service and the HTTPS service: FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#enable service web-server	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.2 http check version

	Use this command to detect the available upgrade files on the HTTP server.
	http check-version

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to detect the available upgrade files. The detected upgrade files version is later than that of local files.	
Configuration Examples	The following example demonstrates the version of the detected HTTP upgrade file. <pre> FS# http check-version Business modules need to be updated: character-db, route-db app name:web app-name version filename ----- character-db 2014.02.09.14.02.09 app_sub_1.exe character-db 2014.02.09.14.02.09 app_file_list.txt character-db 2014.02.09.14.02.09 app_sub_3.exe character-db 2014.02.09.14.02.09 app_sub_2.exe route-db 2013.12.01.00 route-choose.db </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.3 http port

	Use this command to configure the HTTP port number. Use the no form of this command to restore the default HTTP port number.	
	http port <i>port-number</i>	
	no http port	
Parameter Description	Parameter	Description
	<i>port-number</i>	Configures the HTTP port number. The value includes 80, 1025 to 65,535.
Defaults	The default HTTP port number is 80.	

Command mode	Global configuration mode.	
Usage Guide	Use this command to configure the HTTP port number.	
Configuration Examples	The following example configures the HTTP port number as 8080: <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#http port 8080</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.4 http secure-port

	Use this command to configure the HTTPS port number. Use the no form of this command to restore the default HTTPS port number.	
	http secure-port <i>port-number</i>	
	no http secure-port	
Parameter Description	Parameter	Description
	<i>port-number</i>	Configures the HTTPS port number. The value includes 443, 1025 to 65,535.
Defaults	The default HTTP port number is 443.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure the HTTPS port number.	
Configuration Examples	The following example configures the HTTPS port number as 4443: <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#http secure-port 4443</pre>	
Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.
	show web-server status	Displays the configuration and status of the Web

		service.
Platform	N/A	
Description		

7.5 http update

	Use this command to manually upgrade files.	
	http update { all string }	
Parameter Description	Parameter	Description
	<i>string</i>	Name of the service to be upgraded. You can enter multiple services, and separate them with spaces.
	all	Upgrade all services.
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example upgrades the route-db and url-db files. <pre>FS# http update route-db Downloading updated files, please wait... Press Ctrl+C to quit route-db: download and notify successfully.</pre>	
Related Commands	Command	Description
	http check-vesion	Detects the available update package on the HTTP server.
Platform	N/A	
Description		

7.6 http update mode

	Use this command to configure the HTTP upgrade mode to manual mode. Use the no form of this command to restore the default upgrade mode, namely, auto mode.
	http update mode manual
	no http update mode

Parameter Description	Parameter	Description
	manual	Configures the manual upgrade mode.
Defaults	The default update mode is auto mode.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure the HTTP upgrade mode to manual mode.	
Configuration Examples	The following example enables manual HTTP upgrade mode: <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#http update mode manual</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 http update server

	Use this command to configure the IP address and the HTTP port number of the HTTP server.	
	http update server { <i>host-name</i> <i>ip-address</i> } [port <i>port-number</i>]	
	no http update server	
Parameter Description	Parameter	Description
	<i>host-name</i>	Host name of the HTTP server.
	<i>ip-address</i>	IP address of the HTTP server.
	<i>port-number</i>	Port number of the HTTP server. The range is from 1 to 65,535.
Defaults	By default, the IP address of the HTTP remote upgrade server is 0.0.0.0 and the port number is 80.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure the IP address and the HTTP port number of the HTTP server. When processing upgrade, the user-configured server address is preferentially used. If the connection fails, the server address in store in the local upgrade record file will be used to establish the connection. When all the above connection fails, upgrade will be suspended.	

	At least one IP address of upgrade server is stored in the local upgrade record file, and this IP address cannot be modified.  The HTTP upgrade server address is not need to be configured because the local upgrade record file records available upgrade server addresses. If the server domain needs to be configured, enable the DNS function on the device and configure the DNS server address. The server IP address cannot be an IPv6 address.					
Configuration Examples	The following example configures the IP address and the HTTP port number of the HTTP server: <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#http update server 10.83.132.1 port 90</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

7.8 http update set oob

	Use this command to enable HTTP upgrade on the MGMT port. Use the no form of this command to restore the default setting.	
	http update set oob	
	no http update set oob	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, HTTP upgrade is performed on the common port.	
Command mode	Global configuration mode.	
Usage Guide	This command is supported only on the device supporting the MGMT ports.	
Configuration Examples	The following example enables HTTP upgrade on the MGMT port: FS(config)# http update set oob	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.9 http update time

	Use this command to configure the HTTP auto-detection time. Use the no form of this command to restore the default auto-detection time.	
	http update time daily <i>hh:mm</i>	
	no http update time	
Parameter Description	Parameter	Description
	<i>hh:mm</i>	Specified auto-detection time; (24-hour system); accurate to minute.
Defaults	The default HTTP auto-detection time is random.	
Command mode	Global configuration mode.	
Usage Guide	Use this command to configure the HTTP auto-detection time. The device detects the files available for upgrade on the server at the specified detection time. Use can read these detected file information through Web interface. Use the no form of this command to reset the auto-detection time as random.	
Configuration Examples	The following example configures the HTTP auto-detection time. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#http update time daily 23:40</pre>	
Related Commands	Command	Description
	http update mode	Configures the HTTP update mode
Platform Description	N/A	

7.10 show web-server status

	Use this command to display the configuration and status of the Web service.
	show web-server status

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration and status of the Web service: <pre>FS#show web-server status http server status : enabled http server port : 80 https server status: enabled https server port: 443</pre>	
Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.
	http port	Configures the HTTP port number.
	http secure-port	Configures the HTTPS port number.
Platform Description	N/A	

7.11 webmaster level

	Use this command to configure the username and password for Web login authentication. Use the no form of this command to restore the default setting.	
	webmaster level <i>privilege-level</i> username <i>name</i> password { <i>password</i> [0 7] <i>encrypted-password</i> }	
	no webmaster level <i>privilege-level</i> [username <i>name</i>]	
Parameter Description	Parameter	Description
	<i>privilege-level</i>	Configures the user privilege-level.
	<i>name</i>	Username.
	<i>password</i>	Password.
	0 7	Password type; 0 indicates plaintext, 7 indicates ciphertext.
	<i>encrypted-password</i>	Password text.
Defaults	By default, two users are configured. 1. User1 is configured with privilege level 1, username of admin and plaintext password of admin.	

	2. User2 is configured with privilege level 2, username of guest and plaintext password of guest.	
Command mode	Global configuration mode.	
Usage Guide	When HTTP is enabled, users can log in to the Web interface only after being authenticated. Use this command to configure the username and password for Web login authentication. Use the no webmaster level privilege-level command to delete all the usernames and passwords with a specified <i>privilege-level</i>. Use the no webmaster level privilege-level username name command to delete the specified username and password.  Usernames and passwords come with three permission levels, each of which includes at most 10 usernames and passwords.  By default, the system creates the admin account. The account cannot be deleted and only the password of the account can be changed. The administrator account is the admin account, which corresponds to the level 0 permission. The administrator account owns all permissions on the Web page and can edit other management accounts and authorize the accounts to access pages.	
Configuration Examples	The following example configures the username and password for Web login authentication, <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#webmaster level 0 username FS password admin</pre>	
Related Commands	Command	Description
	enable service web-server	Enables the HTTP service.
Platform Description	N/A	

8 Syslog Commands

8.1 clear logging

	Use this command to clear the logs from the buffer in privileged EXEC mode.	
	clear logging	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command clears the log packets from the memory buffer. You cannot clear the statistics of the log packets.	
Configuration Examples	The following example clears the log packets from the memory buffer.	
	FS# clear logging	
Related Commands	Command	Function
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	logging buffered	Records the logs in the memory buffer.
Platform Description	N/A	

8.2 logging

	Use this command to send the log message to the specified syslog server.	
	logging { <i>ip-address</i> ipv6 <i>ipv6-address</i> } [udp-port <i>port</i>] [vrf <i>vrf-name</i>]	
	Use this command to delete the specified syslog server.	
	no logging { <i>ip-address</i> [vrf <i>vrf-name</i>] ipv6 <i>ipv6-address</i> }	
	Use this command to restore the default port 514.	
	no logging { <i>ip-address</i> [vrf <i>vrf-name</i>] ipv6 <i>ipv6-address</i> } udp-port	
Parameter	Parameter	Description
Description	<i>ip-address</i>	Sets the IP address of the host receiving log messages.
	<i>vrf-name</i>	Sets the VRF instance connecting with the host.

	<i>ipv6-address</i>	Sets the IPv6 address of the host receiving log messages.
	udp-port <i>port</i>	Sets the port number of the host receiving log messages. The default is 514.
Defaults	No log message is sent to syslog server by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure a syslog server to receive log messages from the device. You can configure up to five syslog servers, log messages are sent to all configured syslog servers simultaneously,	
Configuration Examples	The following example configures a syslog server with IP address 202.101.11.1. <pre>FS(config)# logging 202.101.11.1</pre> The following example configures a syslog server with IP address 10.1.1.100 and port number 8099. <pre>FS(config)# logging 202.101.11.1 udp-port 8099</pre> The following example configures a syslog server with IPv6 address AAAA:BBBB::FFFF. <pre>FS(config)# logging ipv6 AAAA:BBBB::FFFF</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.3 logging buffered

	Use this command to set the memory buffer parameters (log severity, buffer size) for logs at global configuration layer. Use the no form of the command to disable recording logs in the memory buffer. Use the default form of this command to restore the default setting.	
	logging buffered [<i>buffer-size</i> <i>level</i>]	
	no logging buffered	
	default logging buffered	
Parameter Description	Parameter	Description
	<i>buffer-size</i>	Size of the buffer is related to the specific device type: 1. For the kernel / aggregation switches, 4 K to 10 M bytes. 2. For the access switches, 4 K to 1 M Bytes. 3. For other devices, 4 K to 128 K Bytes.
	<i>level</i>	Severity of logs, from 0 to 7. The name of the severity or the numeral can be used.
Defaults	The buffer size is related to the specific device type. 1. kernel switches: 1 M Bytes;	

	2. aggregation switches: 256 K Bytes; 3. access switches: 128 K Bytes; 4. other devices: 4 K Bytes The log severity is 7.																											
Command Mode	Global configuration mode																											
Usage Guide	The memory buffer for log is used in recycled manner. That is, when the memory buffer with the specified size is full, the oldest information will be overwritten. To show the log information in the memory buffer, run the show logging command in privileged user mode. The logs in the memory buffer are temporary, and will be cleared in case of device restart or the execution of the clear logging command in privileged user mode. To trace a problem, it is required to record logs in flash or send them to Syslog Server. The log information is classified into the following 8 levels (Table 1): Table-1 <table><tr><th>Keyword</th><th>Level</th><th>Description</th></tr><tr><td>Emergencies</td><td>0</td><td>Emergency case, system cannot run normally</td></tr><tr><td>Alerts</td><td>1</td><td>Problems that need immediate remedy</td></tr><tr><td>Critical</td><td>2</td><td>Critical conditions</td></tr><tr><td>Errors</td><td>3</td><td>Error message</td></tr><tr><td>warnings</td><td>4</td><td>Alarm information</td></tr><tr><td>Notifications</td><td>5</td><td>Information that is normal but needs attention</td></tr><tr><td>informational</td><td>6</td><td>Descriptive information</td></tr><tr><td>Debugging</td><td>7</td><td>Debugging messages</td></tr></table> Lower value indicates higher level. That is, level 0 indicates the information of the highest level. When the level of log information to be displayed on devices is specified, the log information at or below the set level will be allowed to be displayed.  After running the system for a long time, modifying the log buffer size especially in condition of large buffer may fails due to the insufficient available continuous memory. The failure message will be shown. It is recommended to modify the log buffer size as soon as the system starts.	Keyword	Level	Description	Emergencies	0	Emergency case, system cannot run normally	Alerts	1	Problems that need immediate remedy	Critical	2	Critical conditions	Errors	3	Error message	warnings	4	Alarm information	Notifications	5	Information that is normal but needs attention	informational	6	Descriptive information	Debugging	7	Debugging messages
Keyword	Level	Description																										
Emergencies	0	Emergency case, system cannot run normally																										
Alerts	1	Problems that need immediate remedy																										
Critical	2	Critical conditions																										
Errors	3	Error message																										
warnings	4	Alarm information																										
Notifications	5	Information that is normal but needs attention																										
informational	6	Descriptive information																										
Debugging	7	Debugging messages																										
Configuration Examples	The following example allows logs at and below severity 6 to be recorded in the memory buffer sized 10,000 bytes. <pre>FS(config)# logging buffered 10000 6</pre>																											

Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs in the buffer.
	clear logging	Clears the logs in the log buffer.
Platform Description	N/A	

8.4 logging console

	Use this command to set the severity of logs that are allowed to be displayed on the console in global configuration mode. Use the no form of this command to prohibit printing log messages on the console.	
	logging console [level]	
	no logging console	
Parameter Description	Parameter	Description
	<i>level</i>	Severity of log messages, 0 to 7. The name of the severity or the numeral can be used. For the details of log severity, see table 1.
Defaults	The default is debugging (7).	
Command Mode	Global configuration mode	
Usage Guide	When a log severity is set, the log messages at or below that severity will be displayed on the console. The show logging command displays the related setting parameters and statistics of the log.	
Configuration Examples	The following example sets the severity of log that is allowed to be displayed on the console as 6: FS(config)# logging console informational	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the logs and related log configuration parameters in the buffer.
Platform Description	N/A	

8.5 logging count

	Use this command to enable the log statistics function in global configuration mode. Use the no form of this command to restore the default setting.	
	logging count	
	no logging count	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The log statistics function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command enables the log statistics function. The statistics begins when the function is enabled. If you run the no logging count command, the statistics function is disabled and the statistics data is deleted.	
Configuration Examples	The following example enables the log statistics function: FS(config)# logging count	
Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.
Platform Description	N/A	

8.6 logging delay-send file

	Use this command to set the name of the log file saved locally for delay sending. Use the no form of this command to restore the default setting.	
	logging delay-send file flash:filename	
	no logging delay-send file	
Parameter Description	Parameter	Description
	flash:filename	Sets the name of the log file saved locally for delay sending.
Defaults	The default name format is as follows: file size_device IP address_index.txt. If you want to change the file name, the file sent to the remote server should be named as follows: prefix_ file size_device IP address_index.txt; the file saved locally should be named as follows: prefix_index.txt. The default prefix is syslog_ftp_server.	
Command Mode	Global configuration mode	
Usage Guide	The file name cannot contain special symbols including . \ : * " < > and . For example, the file name is log_server, file index 5, file size 1000B and device IP address 10.2.3.5. The log file	

	sent to the remote server is named log_server_1000_10.2.3.5_5.txt and the log file saved locally is named log_server_5.txt. If the device has an IPv6 address, the colon (:) in the IPv6 address is replaced by the hyphen (-). For example, the is log_server, file index 6, file size 1000B and device IPv6 address 2001::1. The log file sent to the remote server is named log_server_1000_2001-1_6.txt and the log file saved locally is named log_server_6.txt.	
Configuration Examples	The following example sets the name of the log file saved locally to log_server. <pre>FS(config)# logging delay-send file flash:log_server</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.7 logging delay-send interval

	Use this command to set the interval at which log sending is delayed. Use the no form of this command to restore the default setting.	
	logging delay-send interval <i>seconds</i>	
	no logging delay-send interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the interval at which log sending is delayed, in the range from 600 to 65535 seconds.
Defaults	The default is 3600.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the the interval at which log sending is delayed to 600 seconds. <pre>FS(config)# logging delay-send interval 600</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

8.8 logging delay-send server

	Use this command to set the interval at which log sending is delayed. Use the no form of this command to restore the default setting.	
	logging delay-send interval <i>seconds</i>	
	no logging delay-send interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the interval at which log sending is delayed, in the range from 600 to 65535 seconds.
Defaults	The default is 3600.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the the interval at which log sending is delayed to 600 seconds. <pre>FS(config)# logging delay-send interval 600</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.9 logging delay-send terminal

	Use this command to enable delay in sending logs to console and remote terminal. Use the no form of this command to restore the default setting.	
	logging delay-send terminal	
	no logging delay-send terminal	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables delay in sending logs to console and remote terminal. <pre>FS(config)# logging delay-send terminal</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.10 logging facility

	Use this command to configure the device value of the log information in global configuration mode. Use the no form of the command to restore the default setting.																	
	logging facility facility-type																	
	no logging facility																	
Parameter	Parameter	Description																
Description	facility-type	Syslog device value. For specific settings, refer to the usage guide.																
Defaults	The default is 23 if the RFC5424 format is enabled (Local7, local use). The default is 16 if the RFC5424 format is disabled (Local0, local use).																	
Command Mode	Global configuration mode																	
Usage Guide	The following table (Table-2) is the possible device values of Syslog: <table><tr><th>Numerical Code</th><th>Facility</th></tr><tr><td>0 (kern)</td><td>Kernel messages</td></tr><tr><td>1 (user)</td><td>User-level messages</td></tr><tr><td>2 (mail)</td><td>Mail system</td></tr><tr><td>3 (daemon)</td><td>System daemons</td></tr><tr><td>4 (auth1)</td><td>security/authorization messages</td></tr><tr><td>5 (syslog)</td><td>Messages generated internally by syslogd</td></tr><tr><td>6 (lpr)</td><td>Line printer subsystem</td></tr></table>		Numerical Code	Facility	0 (kern)	Kernel messages	1 (user)	User-level messages	2 (mail)	Mail system	3 (daemon)	System daemons	4 (auth1)	security/authorization messages	5 (syslog)	Messages generated internally by syslogd	6 (lpr)	Line printer subsystem
Numerical Code	Facility																	
0 (kern)	Kernel messages																	
1 (user)	User-level messages																	
2 (mail)	Mail system																	
3 (daemon)	System daemons																	
4 (auth1)	security/authorization messages																	
5 (syslog)	Messages generated internally by syslogd																	
6 (lpr)	Line printer subsystem																	

	7 (news)	USENET news
	8 (uucp)	Unix-to-Unix copy system
	9 (clock1)	Clock daemon
	10 (auth2)	security/authorization messages
	11 (ftp)	FTP daemon
	12 (ntp)	NTP subsystem
	13 (logaudit)	log audit
	14 (logalert)	log alert
	15 (clock2)	clock daemon
	16 (local0)	Local use
	17 (local1)	Local use
	18 (local2)	Local use
	19 (local3)	Local use
	20 (local4)	Local use
	21 (local5)	Local use
	22 (local6)	Local use
	23 (local7)	Local use
The default device value of FSOS is 23 (local 7).		
Configuration Examples	The following example sets the device value of Syslog as kernel : FS(config)# logging facility kern	
Related Commands	Command	Description
	logging console	Sets the severity of logs that are allowed to be displayed on the console.
Platform Description	N/A	

8.11 logging file

	Use this command to save log messages in the log file, which can be saved in hardware disk, expanded FLASH, USB or SD. Use the no form of this command to restore the default setting,	
	logging file { sata0:filename flash:filename flash2:filename usb0:filename usb1:filename sd0:filename } [<i>max-file-size</i>] [<i>level</i>]	
	no logging file	
Parameter Description	Parameter	Description
	sata0	Saves the log file in hardware disk.

	flash	Saves the log file in expanded FLASH.																											
	flash2	Saves the log file in expanded FLASH2.																											
	usb0	Saves the log file in USB0. This parameter is supported by the device with one USB connector and the USB extension device.																											
	usb1	Saves the log file in USB1. This parameter is supported by the device with two USB connectors and the USB extension device.																											
	sd0	Saves the log file in the SD card. This parameter is supported by the device with the SD card interface and the SD card extension device.																											
	filename	Sets the file name. The file type is omitted, which is fixed as txt.																											
	max-file-size	Sets the maximum file size, in the range from 128K to 6M bytes. The default is 128K.																											
	level	Sets the level of the log message saved in the log file, which can be either the level name or the level number. The default is 6. See Usage Guide for details.																											
Defaults	Log messages are not saved in expanded FLASH by default.																												
Command Mode	Global configuration mode																												
Usage Guide	You can save log messages in expanded FLASH if you don't want to transmit log messages on the network or there is no syslog server. The log file cannot be configured with the suffix, which is fixed as txt.  If there is no expanded FLASH, the logging file flash command is hidden automatically and cannot be configured. If no FLASH2 is available, the logging file flash command is hidden automatically and cannot be configured. If FLASH2 is available, the log file is saved in FLASH2 after the logging file flash command is configured. <table border="1"> <thead> <tr> <th>Keyword</th><th>Level</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Emergencies</td><td>0</td><td>Emergency case. The system fails to run.</td></tr> <tr> <td>Alerts</td><td>1</td><td>Problem that call for immediate solution.</td></tr> <tr> <td>Critical</td><td>2</td><td>Critical message.</td></tr> <tr> <td>Errors</td><td>3</td><td>Error message.</td></tr> <tr> <td>warnings</td><td>4</td><td>Alarm message.</td></tr> <tr> <td>Notifications</td><td>5</td><td>message that is normal but calls for attention.</td></tr> <tr> <td>informational</td><td>6</td><td>Descriptive message.</td></tr> <tr> <td>Debugging</td><td>7</td><td>Debugging message</td></tr> </tbody> </table>		Keyword	Level	Description	Emergencies	0	Emergency case. The system fails to run.	Alerts	1	Problem that call for immediate solution.	Critical	2	Critical message.	Errors	3	Error message.	warnings	4	Alarm message.	Notifications	5	message that is normal but calls for attention.	informational	6	Descriptive message.	Debugging	7	Debugging message
Keyword	Level	Description																											
Emergencies	0	Emergency case. The system fails to run.																											
Alerts	1	Problem that call for immediate solution.																											
Critical	2	Critical message.																											
Errors	3	Error message.																											
warnings	4	Alarm message.																											
Notifications	5	message that is normal but calls for attention.																											
informational	6	Descriptive message.																											
Debugging	7	Debugging message																											
Configuration Examples	The following example saves the log message in expanded FLASH and sets file name, file size and log level to syslog.txt, 128K and 6 respectively. <pre>FS(config)# logging file flash:syslog</pre>																												

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.12 logging file numbers

	Use this command to set the number of log files written into FLASH. Use the no form of this command to restore the default setting.	
	logging file numbers <i>numbers</i>	
	no logging file numbers	
Parameter Description	Parameter	Description
	<i>numbers</i>	Sets the number of log files written into FLASH, in the range from 2 to 16.
Defaults	The default is 16.	
Command Mode	Global configuration mode	
Usage Guide	The system does not delete previously generated log files even if you change this configuration, Therefore, you need to delete the log files manually to save FLASH size (you can send log files to the server through TFTP before that). For example, 16 log files are generated by default before you want to change the number to 2. New logs are overwritten constantly in log files indexed 0 to 1. However, log files indexed from 2 to 16 remain. You can delete these log files manually as needed.	
Configuration Examples	The following example sets the number of log files written into FLASH to 8. FS(config)# logging file numbers 8	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.13 logging filter direction

	Use this command to filter the log messages destined to a certain direction. Use the no form of this command to restore the default setting.	
	logging filter direction { all buffer file server terminal }	
	no logging filter direction { all buffer file server terminal }	
Parameter Description	Parameter	Description
	all	Log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server.
	buffer	Log messages destined to the log buffer are filtered, including log messages displayed by running the show logging command.
	file	Log messages destined to the log file are filtered.
	server	Log messages destined to the log server are filtered.
	terminal	Log messages destined to the console and the VTY terminal (including Telnet and SSH).
Defaults	Log messages destined to all directions are filtered by default.	
Command Mode	Global configuration mode	
Usage Guide	In general, log messages destined to all directions are filtered, including console, VTY terminal, log buffer, log file and log server. If you want to filter log messages destined to a certain direction, the terminal for instance, configure the terminal parameter.	
Configuration Examples	The following example filters log messages destined to the terminal (including the console and the VTY terminal). FS(config)# logging filter direction terminal	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.14 logging filter rule

	Use this command to configure the filter rule of the log message,	
	logging filter rule { exact-match module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i> single-match [level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i>] }	
	Use this command to delete the "exact-match" filter rule.	
	no logging filter rule exact-match [module <i>module-name</i> mnemonic <i>mnemonic-name</i> level <i>level</i>]	

	Use this command to delete the “single-match” filter rule.	
	no logging filter rule single-match [level <i>level</i> mnemonic <i>mnemonic-name</i> module <i>module-name</i>]	
Parameter Description	Parameter	Description
	exact-match	Exact-match filter rule. Fill in all the following three parameters.
	single-match	Single-match filter rule. Fill in one of the following three parameters.
	module <i>module-name</i>	Module name.
	mnemonic <i>mnemonic-name</i>	Mnemonic name.
	level <i>level</i>	Log level,
Defaults	No filter rule is configured by default,	
Command Mode	Global configuration mode	
Usage Guide	If you want to filter a specific log message, use the “exact-match” filter rule and fill in all three parameters, namely, module name, mnemonic name and log level. If you want to filter a specific kind of log messages, use the “single-match” filter rule and fill in one of three parameters, namely, module name, mnemonic name and log level. When configured with the same module name, mnemonic name or log level, the “single-match” filter rule has a higher priority than the “exact-match” filter rule,	
Configuration Examples	The following example configures the “exact-match” filter rule with parameters of module name LOGIN, log level 5 and mnemonic name LOGOUT. <pre>FS(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5</pre> The following example configures the “single-match” filter rule with the parameter of module name SYS. <pre>FS(config)# logging filter rule single-match module SYS</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.15 logging filter type

	Use this command to configure the filter type of log messages. Use the no form of this command to restore the default setting.	
	logging filter type { contains-only filter-only }	
	no logging filter type	

Parameter Description	Parameter	Description
	contains-only	The log message containing the key word of the filter rule is printed.
	filter-only	The log message containing the key word of the filter rule is filtered.
Defaults	The default filter type is filter-only.	
Command Mode	Global configuration mode	
Usage Guide	- When too many log messages are printed, the terminal screen keeps being refreshed. If you are not concerned with these log messages, use the "filter-only" filter type to filter the log messages, - If you are concerned with certain log messages, use the "contains-only" filter type to print log messages containing the key word of the filter rule, so as to monitor whether certain events happen.  In real operation, the contains-only and the filter-only filter types cannot be configured at the same time.  If you configure the filter direction and the filter type without configuring the filter rule, the log messages are not filtered.	
Configuration Examples	The following example sets the filter type to contains-only. <pre>FS(config)# logging filter type contains-only</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.16 logging flash flush

	Use this command to write log messages in the system buffer into the flash file immediately.	
	logging flash flush	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	In general, the log messages are cached in the log buffer. Only when the buffer is full or the timer expires are log	

	messages written into the flash file. This command is used to write log messages in the system buffer into the flash file immediately.  The logging flash flush command takes effect only once for each configuration. The log messages cached in the buffer are written into the flash file immediately after configuration.					
Configuration Examples	The following example writes log messages in the system buffer into the flash file immediately. <pre>FS(config)# logging flash flush</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

8.17 logging flash interval

	Use this command to set the interval to write log messages into the flash file, Use the no form of this command to restore the default setting.	
	logging flash interval <i>seconds</i>	
	no logging flash interval	
Parameter Description	Parameter	Description
	interval <i>seconds</i>	The interval to write log messages into the flash file, in the range from 1 to 57840 in the unit of seconds.
Defaults	The default is 3600.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to set the interval to write log messages into the flash file. The timer starts after configuration, If you want to restore the interval to 3600 seconds, use the no logging flash interval command.  To avoid writing log messages into the flash file too frequently, it is not recommended to set a short interval.	
Configuration Examples	The following example sets the interval to write log messages into the flash file to 300 seconds.	
	FS(config)# logging flash interval 300	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.18 logging life-time

	Use this command to configure the preservation duration of logs in expanded FLASH. Use the no form of this command to restore the default setting.	
	logging life-time level level days	
	no logging life-time level level	
Parameter Description	Parameter	Description
	<i>level</i>	Sets the log level, which can be either the level name or the level number.
	<i>days</i>	Sets the preservation duration of logs.
Defaults	No preservation duration is set by default.	
Command Mode	Global configuration mode	
Usage Guide	Due to difference in expanded FLASH size and log level, logs with different levels can be configured with different preservation durations.  Once log preservation based on time is enabled, log preservation based on file size is disabled automatically. The log files are stored under the syslog/ directory of the expanded FLASH,	
Configuration Examples	The following example sets the preservation duration of logs whose level is 6 to 10 days. <pre>FS(config)# logging life-time level 6 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.19 logging monitor

	Use this command to set the severity of logs that are allowed to be displayed on the VTY window (telnet window, SSH window, etc.) in global configuration mode. Use the no form of this command to disable this function.
	logging monitor [level]

	no logging monitor	
Parameter	Parameter	Description
Description	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table-1.
Defaults	The default is debugging (7).	
Command Mode	Global configuration mode	
Usage Guide	To print log information on the VTY window, run the terminal monitor command in privileged EXEC mode. The level of logs to be displayed is defined by logging monitor. The log level defined with "Logging monitor" is for all VTY windows.	
Configuration Examples	The following example sets the severity of log that is allowed to be printed on the VTY window as 6: <pre>FS(config)# logging monitor informational</pre>	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays the log messages and related log configuration parameters in the buffer.
Platform Description	N/A	

8.20 logging on

	Use this command globally to allow logs to be displayed on different devices. Use the no form of this command to disable this function.	
	logging on	
	no logging on	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	Logs are allowed to be displayed on different devices.	
Command Mode	Global configuration mode	
Usage Guide	Log information can not only be shown in the Console window and VTY window, but also be recorded in	

	different equipments such as the memory buffer, the expanded FLASH and the Syslog Server. This command is the total log switch. If this switch is turned off, no log will be displayed or recorded unless the severity level is smaller than 1.	
Configuration Examples	The following example disables the log switch on the device.	
	FS(config)# no logging on	
Related Commands	Command	Description
	logging buffered	Records the logs to a memory buffer.
	logging server	Sends logs to the Syslog server.
	logging file flash:	Records logs on the expanded FLASH.
	logging console	Allows the log level to be displayed on the console.
	logging monitor	Allows the log level to be displayed on the VTY window (such as telnet window) .
	logging trap	Sets the log level to be sent to the Syslog server.
Platform Description	N/A	

8.21 logging policy

	Use this command to configure the severity ranking policy. Use the no form of this command to remove one policy, Use the no logging policy command to remove all policies.	
	logging policy module <i>module-name</i> [not-lesser-than] <i>level</i> direction { all server file console monitor buffer }	
	no logging policy module <i>module-name</i> [not-lesser-than] <i>level</i> direction { all server file console monitor buffer }	
	no logging policy	
Parameter Description	Parameter	Description
	<i>module-name</i>	The name of the module applying the ranking policy.
	not-lesser-than	If this parameter is specified, only when the log's level is not lower than the configured level can the log be sent. Otherwise, the log is filtered. If this parameter is not specified, only when the log's level is not higher than the configured level can the log be sent. Otherwise, the log is filtered.
	<i>level</i>	Severity level
	all	Applies the ranking policy in all directions.
	server	Applies the ranking policy to the direction toward the server.
	file	Applies the ranking policy to the direction toward the log file.
	console	Applies the ranking policy to the direction toward the console.
	monitor	Applies the ranking policy to the direction toward the remote server.
	buffer	Applies the ranking policy to the direction toward the buffer.

Defaults	This function is disabled by default.				
Command Mode	Global configuration mode				
Usage Guide	This command is used to send logs to different destinations based on module and severity.				
Configuration Examples	The following example sends logs of the SYS module leveled above 5 to the console and sends logs of the SYS module leveled below 3 to the buffer. <pre>FS(config)# logging policy module SYS not-less-than 5 direction console FS(config)# logging policy module SYS 3 direction buffer</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

8.22 logging rate-limit

	Use this command to enable log rate limit function to limit the output logs in a second in the global configuration mode. Use the no form of this command to disable this function.	
	logging rate-limit { number all number console { number all number } } [except severity]	
	no logging rate-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The number of logs that can be processed in a second in the range from 1 to 10000.
	all	Sets rate limit to all the logs with severity level 0 to 7.
	console	Sets the amount of logs that can be shown in the console in a second.
	except	By default, the severity level is error (3). The rate of the log whose severity level is less than or equal to error (3) is not controlled.
	<i>severity</i>	Log severity level in the range from 0 to 7. The lower the level is, the higher the severity is.
Defaults	The log rate limit function is disabled by default.	
Command Mode	Global configuration mode	

Usage Guide	Use this command to control the syslog output to prevent the massive log output.	
Configuration Examples	The following example sets the number of the logs (including debug) that can be processed in a second as 10. However, the logs with warning or higher severity level are not controlled: FS(config)#logging rate-limit all 10 except warnings	
Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.
Platform Description	N/A	

8.23 logging rd on

	Use this command in global configuration mode on the host to enable the log re-direction function and allow re-directing logs on slave or backup devices to the host in the stacking environment. Use no form of this command to disable this function.	
	logging rd on	
	no logging rd on	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The log re-direction function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The log information on slave or back devices not only can be shown on the Console window of slave or backup devices, but also can be re-directed to the host and exported to the Console and VTY windows of the host, and recorded in cache, expanded FLASH and Syslog Server of the host.	
Configuration Examples	The following example enables the log re-direction function on a device: FS(config)#logging rd on	
Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.

Platform Description	N/A

8.24 logging rd rate-limit

	Use this command in global configuration mode on the host to enable the log re-direction rate limiting function to limit the number of logs that can be re-directed from a slave or backup device to the host each second in the stacking environment. Use the no form of this command to disable this function. logging rd rate-limit <i>number</i> [except [<i>severity</i>]] no logging rd rate-limit	
Parameter Description	Parameter	Description
	<i>number</i>	Log information that can be re-directed each second, ranging from 1 to 10,000 logs
	except	Log information on or lower than the severity level will not be limited; error (3) by default, log information on or lower than the error level is not limited.
	<i>severity</i>	Log information severity level; lower the level is, higher the severity is, ranging from 0 to 7
Defaults	The maximum number of logs that can be re-directed each second is 200 by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to control the output of log information by system re-direction. You can use this command to prevent a slave or backup device from re-directing a large number of logs to the host.	
Configuration Examples	The following example sets the maximum number of logs (including debug) that can be re-directed from a slave device to the host each second at 10, excepting logs on and above the warning severity level: <pre>FS(config)#logging rd rate-limit 10 except warnings</pre>	
Related Commands	Command	Description
	show logging count	Displays log information about modules of the system.
	show logging	Displays basic configuration of log modules and log information in the buffer.
Platform Description	N/A	

8.25 logging server

	Use this command to send the logs to the specified Syslog Sever in global configuration mode. Use the no form of this command to remove the setting. Use the default form of this command to restore the default setting.

	logging server [oob] { ip-address ipv6 ipv6-address } [udp-port port] [vrf vrf-name] no logging server [oob] { ip-address [vrf vrf-name] ipv6 ipv6-address } no logging server { ip-address [vrf vrf-name] ipv6 ipv6-address } udp-port	
Parameter Description	Parameter	Description
	oob	Specifies out-of-band communication for the logging server. (logs are sent through the MGMT port to the logging server.)
	ip-address	IP address of the host that receives log information.
	vrf-name	Specifies the VRF instance (VPN device forwarding table) connecting to the log host.
	ipv6-address	Specifies IPV6 address for the host receiving the logs.
	udp-port port	Specifies the port number for the specified host (The default port number is 514).
Defaults	No log is sent to any syslog server by default.	
Command Mode	Global configuration mode	
Usage Guide	This command specifies a Syslog server to receive the logs of the device. Users are allowed to configure up to 5 Syslog Servers. The log information will be sent to all the configured Syslog Servers at the same time. The via parameter is available only after the oob parameter is used. The /vrf parameter cannot be used at the same time. The IPv6 server does not support VRF and oob.	
Configuration Examples	The following example specifies a syslog server of the address 202.101.11.1: FS(config)# logging server 202.101.11.1 The following example specifies an ipv6 address as AAAA:BBBB:FFFF: FS(config)# logging server ipv6 AAAA:BBBB:FFFF	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	show logging	Displays log messages and related log configuration parameters in the buffer.
	logging trap	Sets the level of logs allowed to be sent to Syslog server.
Platform Description	N/A	

8.26 logging source interface

	Use this command to configure the source interface of logs in global configuration mode. Use the no form of this command to restore the default setting.

	logging source [interface] interface-type interface-number no logging source [interface]	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.
Defaults	No source interface is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an interface address, so that the administrator can identify which device is sending the message through the unique addresses. If the source interface is not configured on the device, or no IP address is configured for the source interface, the source address of the log messages is the address of the sending interface.	
Configuration Examples	The following example specifies loopback 0 as the source address of the syslog messages: FS(config)# logging source interface loopback 0	
Related Commands	Command	Description
	logging server	Sends logs to the Syslog server.
Platform Description	N/A	

8.27 logging source ip | ipv6

	Use this command to configure the source IP address of logs in global configuration mode. Use the no form of this command to restore the default setting. logging source {ip ip-address ipv6 ipv6-address} no logging source { ip ipv6 }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the source IPV4 address sending the logs to IPV4 log server.
	<i>ipv6-address</i>	Specifies the source IPV6 address sending the logs to IPV6 log server.
Defaults	No source address is configured by default.	

Command Mode	Global configuration mode	
Usage Guide	By default, the source address of the log messages sent to the syslog server is the address of the sending interface. For easy tracing and management, this command can be used to fix the source address of all log messages as an address, so that the administrator can identify which device is sending the message through the unique addresses. If this IP address is not configured on the device, the source address of the log messages is the address of the sending interface.	
Configuration Examples	The following example specifies 192.168.1.1 as the source address of the syslog messages: FS(config)# logging source ip 192.168.1.1	
Related Commands	Command	Description
	logging server	Sends the logs to the Syslog server.
Platform Description	N/A	

8.28 logging statistic enable

	Use this command to enable logging periodically. Use no form of this command to restore the default setting.	
	logging statistic enable	
	no logging statistic enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to send performance statistics at a certain interval for the server to monitor the system performance.	
Configuration Examples	The following example enables logging periodically. FS(config)# logging statistic enable	
Related Commands	Command	Description
	N/A	N/A

Platform Description	N/A

8.29 logging statistic interval

	Use this command to configure the interval at which logs are sent. Use the no form of this command to restore the default setting.	
	logging statistic mnemonic <i>mnemonic</i> interval <i>minutes</i>	
	no logging statistic mnemonic <i>mnemonic</i>	
Parameter Description	Parameter	Description
	<i>mnemonic</i>	Sets the mnemonics to identify the object.
	<i>minutes</i>	Sets the interval at which logs are sent, in the unit of minutes.
Defaults	The default is 15.	
Command Mode	Global configuration mode	
Usage Guide	The available settings include 0, 15, 30, 60 and 120. 0 indicates this function is disabled.	
Configuration Examples	The following example set the interval at which logs are sent to 30 minutes. <pre>FS(config)# logging statistic mnemonic TUNNEL_STAT interval 30</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.30 logging statistic terminal

	Use this command to enable logs to be sent to the console and the remote terminal periodically. Use the no form of this command to restore the default setting.	
	logging statistic terminal	
	no logging statistic terminal	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enable logs to be sent to the console and the remote terminal. <pre>FS(config)# logging statistic terminal</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.31 logging synchronous

	Use this command to enable synchronization function between user input and log output in line configuration mode to prevent interruption when the user is keying in characters. Use the no form of this command to restore the default setting.	
	logging synchronous	
	no logging synchronous	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The synchronization function between user input and log output is disabled by default.	
Command Mode	Line configuration mode	
Usage Guide	This command enables synchronization function between user input and log output, preventing the user from interrupting when keying in the characters. Print UP-DOWN logs on the port when keying in the command, the input command will be output again: <pre>FS# configure terminal Oct 9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down Oct 9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN FS# configure terminal//----the input command by the user is output again rather than being intererupted.</pre>	

Configuration	FS(config)# line console 0	
Examples	FS(config-line)#logging synchronous	
Related Commands	Command	Description
	show running-config	Displays the configuration.
Platform Description	N/A	

8.32 logging trap

	Use this command to set the severity of logs that are allowed to be sent to the syslog server in global configuration mode. Use the no form of this command to prohibit sending log messages to the Syslog server.	
	logging trap [level]	
	no logging trap	
Parameter Description	Parameter	Description
	<i>level</i>	Severity of the log message. The name of the severity or the numeral can be used. For the details of log severity, see Table 1.
Defaults	The default is informational(6)	
Command Mode	Global configuration mode	
Usage Guide	To send logs to the Syslog Server, run the logging command in global configuration mode to configure the Syslog Server . Then, run the logging trap command to specify the severity level of logs to be sent. The show logging command displays the configured related parameters and statistics of the log.	
Configuration Examples	The following example enables logs at severity 6 to be sent to the Syslog Server with the address of 202.101.11.22: <pre>FS(config)# logging 202.101.11.22 FS(config)# logging trap informational</pre>	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	logging	Sends logs to the Syslog server.
	show logging	Displays the log messages and related log configuration parameters in the buffer.
Platform Description	N/A	

8.33 logging userinfo

	Use this command to enable the logging function to record user log/exit. Use the no form of this command to restore the default setting.	
	logging userinfo	
	no logging userinfo	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No log message is printed recording user log/exit by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to print the log message to remind the administrator of user login. The log message is in the format as follows: <pre>Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.</pre>	
Configuration Examples	The following example enables the logging function to record user log/exit. <pre>FS(config)# logging user-info</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.34 logging userinfo command-log

	Use this command to enable the logging function to record user operation. Use the no form of this command to restore the default setting.	
	logging userinfo command-log	
	no logging userinfo command-log	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No log message is printed recording user operation by default.	
Command	Global configuration mode	

Mode		
Usage Guide	This command is used to print the log message to remind the administrator of configuration change. The log message is in the format as follows: Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log: logging server 192.168.23.68.	
Configuration Examples	The following example enables the logging function to record user operation. FS(config)# logging user-info command-log	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.35 service log-format rfc5424

	Use this command to enable the RFC5424 format. Use the no form of this command to restore the default setting.	
	service log-format rfc5424	
	no service log-format rfc5424	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The RFC3164 format is used by default.	
Command Mode	Global configuration mode	
Usage Guide	After the RFC5424 format is enabled, the service sequence-numbers, service sysname, service timestamps, service private-syslog and service standard-syslog commands become invalid and hidden. After switching back to the RFC3164 format, the logging delay-send, logging policy and logging statistic commands become invalid and hidden. After switching the log format, the results of running the show logging and show logging config commands change,	
Configuration Examples	The following example enables the RFC5424 format.	
	FS(config)# service log-format rfc5424	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.36 service private-syslog

	Use this command to set the syslog format to the private syslog format. Use the no form of this command to restore the default setting.	
	service private-syslog	
	no service private-syslog	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The syslog is displayed in the default format.	
Command Mode	Global configuration mode	
Usage Guide	By default, the syslog is displayed in the format as follows: *timestamp: %facility-severity-mnemonic: description Here is an example: *May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console With this function enabled, the syslog is displayed in the format as follows: timestamp facility-severity-mnemonic: description Here is an example: May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console The difference between the private syslog format and the default syslog format lies in the following marks: The private syslog does not have "*" before the timestamp, ":" after the timestamp and "%" before the identifying string.	
Configuration Examples	The following example sets the private syslog format. <pre>FS(config)# service private-syslog</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.37 service sequence-numbers

	Use this command to attach serial numbers into the logs in global configuration mode. Use the no form of this command to restore the default setting.	
	service sequence-numbers	
	no service sequence-numbers	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	No serial number is contained in the logs by default.	
Command Mode	Global configuration mode	
Usage Guide	In addition to the timestamp, you can add serial numbers to the logs, numbering from 1. Then, it is clearly known whether the logs are lost or not and their sequence.	
Configuration Examples	The following example adds serial numbers to the logs. FS(config)# service sequence-numbers	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	service timestamps	Attaches timestamps to the logs.

Platform N/A
Description

8.38 service standard-syslog

	Use this command to set the syslog format to the standard syslog format defined in RFC3164. Use the no form of this command to restore the default setting.	
	service standard-syslog	
	no service standard-syslog	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The syslog is displayed in the default format.	
Command	Global configuration mode	

Mode						
Usage Guide	By default, the syslog is displayed in the format as follows: <pre>*timestamp: %facility-severity-mnemonic: description</pre> Here is an example: <pre>*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console</pre> With this function enabled, the syslog is displayed in the format as follows: <pre>timestamp %facility-severity-mnemonic: description</pre> Here is an example: <pre>May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console</pre> The difference between the standard syslog format and the default syslog format lies in the following marks: The standard syslog does not have "*" before the timestamp and ":" after the timestamp.					
Configuration Examples	The following example sets the standard syslog format. <pre>FS(config)# service standard-syslog</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

8.39 service sysname

	Use this command to attach system name to logs in global configuration mode. Use the no form of this command to restore the default setting.	
	service sysname	
	no service sysname	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No system name is attached to logs by default.	
Command Mode	Global configuration mode	
Usage Guide	This command allows you to decide whether to add system name in the log information.	
Configuration Examples	The following example adds a system name in the log information: Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console	

	FS #config terminal Enter configuration commands, one per line. End with CNTL/Z. FS (config)#service sysname FS (config)#end FS # Mar 22 15:35:57 S3250 %SYS-5-CONFIG: Configured from console by console	
Related Commands	Command	Function
	show logging	Displays basic configuration of log modules and log information in the buffer.
Platform Description	N/A	

8.40 service timestamps

	Use this command to attach timestamp into logs in global configuration mode. Use the no form of this command to remove the timestamp from the logs. Use the default form of this command to restore the default setting.	
	service timestamps [message-type [uptime datetime [msec year]]]	
	no service timestamps [message-type]	
	default service timestamps [message-type]	
Parameter Description	Parameter	Description
	<i>message-type</i>	The log type, including Log and Debug . The log type indicates the log information with severity levels of 0 to 6. The debug type indicates that with severity level 7.
	uptime	Device start time in the format of *Day*Hour*Minute*Second, for example, 07:00:10:41.
	datetime	Current time of the device in the format of Month*Date*Hour*Minute*Second, for example, Jul 27 16:53:07.
	msec	Current time of the device in the format of Month*Date*Hour*Minute*Second*milisecond, for example, Jul 27 16:53:07.299
	year	Current time of the device in the format of Year*Month*Date*Hour*Minute*Second, for example, 2007 Jul 27 16:53:07
Defaults	The time stamp in the log information is the current time of the device. If the device has no RTC, the time stamp is automatically set to the device start time.	
Command Mode	Global configuration mode	

Usage Guide	When the uptime option is used, the time format is the running period from the last start of the device to the present time, in seconds. When the datetime option is used, the time format is the date of the current device, in the format of YY-MM-DD, HH:MM:SS.	
Configuration Examples	The following example enables the timestamp for log and debug information, in format of Datetime, supporting millisecond display. <pre>FS(config)# service timestamps debug datetime msec FS(config)# service timestamps log datetime msec FS(config)# end FS(config)# Oct 8 23:04:58.301 %SYS-5-CONFIG I: configured from console by console</pre>	
Related Commands	Command	Description
	logging on	Turns on the log switch.
	service sequence-numbers	Enables serial numbers of logs.
Platform Description	N/A	

8.41 show logging

	Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from before to now.	
	show logging	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following command displays the result of the show logging command with RFC5424 format disabled. <pre>FS# show logging Syslog logging: enabled Console logging: level debugging, 15495 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 15496 messages logged Standard format: false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable</pre>	

Sysname log messages: enable

Count log messages: enable

Trap logging: level informational, 15242 message lines logged,0 fail

logging to 202.101.11.22

logging to 192.168.200.112

Log Buffer (Total 131072 Bytes): have written 1336,

015487: *Sep 19 02:46:13: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.

015488: *Sep 19 02:46:13: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.

015489: *Sep 19 02:46:26: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.

015490: *Sep 19 02:46:26: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to down.

015491: *Sep 19 02:46:28: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.

015492: *Sep 19 02:46:28: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.

Log information description:

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging** command with RFC5424 format enabled.

FS# show logging

Syslog logging: enabled

Console logging: level debugging, 4740 messages logged

Monitor logging: level debugging, 0 messages logged

Buffer logging: level debugging, 4745 messages logged

```

Statistic log messages: disable
Statistic log messages to terminal: disable
Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds
Count log messages: enable
Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to 192.168.23.89
    logging to 2000::1
Delay-send logging: 2641 message lines logged
    logging to 192.168.23.89 by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z FS - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z FS - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:32.250265Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<134>1 2013-07-24T12:29:33.410123Z FS SYS 6 SHELL_LOGIN [USER@4881 name="" type="" from="console"]
user login success.
<134>1 2013-07-24T12:29:34.343763Z FS SYS 6 SHELL_CMD [USER@4881 name=""] [CMD@4881 task="rl_con"
cmd="enable"]

```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending mode and statistics
Log Buffer	Log files recorded in the memory buffer

Related Commands	Command	Function
	logging on	Turns on the log switch.
	clear logging	Clears the log messages in the buffer.
Platform Description	N/A	

8.42 show logging config

	Use this command to display log configuration and statistics.																	
	show logging config																	
Parameter Description	Parameter	Description																
	N/A	N/A																
Defaults	N/A																	
Command Mode	Privileged EXEC mode																	
Usage Guide	N/A																	
Configuration Examples	The following example displays the outcome of running the show logging config command with RFC5424 disabled. FS# show logging config Syslog logging: enabled Console logging: level debugging, 15495 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 15496 messages logged Standard format: false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 15242 message lines logged,0 fail logging to 202.101.11.22 logging to 192.168.200.112 <table><tr><th>Field</th><th>Description</th></tr><tr><td>Syslog logging</td><td>Whether the logging function is enabled or disabled.</td></tr><tr><td>Console logging</td><td>The level and statistics of the log message printed on the console.</td></tr><tr><td>Monitor logging</td><td>The level and statistics of the log message printed on the VTY window.</td></tr><tr><td>Buffer logging</td><td>The level and statistics of the log message recorded in the memory buffer.</td></tr><tr><td>Standard format</td><td>Standard log format.</td></tr><tr><td>Timestamp debug messages</td><td>Timestamp format of debugging message.</td></tr><tr><td>Timestamp log messages</td><td>Timestamp format of log message.</td></tr></table>		Field	Description	Syslog logging	Whether the logging function is enabled or disabled.	Console logging	The level and statistics of the log message printed on the console.	Monitor logging	The level and statistics of the log message printed on the VTY window.	Buffer logging	The level and statistics of the log message recorded in the memory buffer.	Standard format	Standard log format.	Timestamp debug messages	Timestamp format of debugging message.	Timestamp log messages	Timestamp format of log message.
Field	Description																	
Syslog logging	Whether the logging function is enabled or disabled.																	
Console logging	The level and statistics of the log message printed on the console.																	
Monitor logging	The level and statistics of the log message printed on the VTY window.																	
Buffer logging	The level and statistics of the log message recorded in the memory buffer.																	
Standard format	Standard log format.																	
Timestamp debug messages	Timestamp format of debugging message.																	
Timestamp log messages	Timestamp format of log message.																	

Sequence-number log messages	Whether the sequence number function is enabled or disabled.
Sysname log messages	Adds the system name to the log message.
Count log messages	Log-counting function
Trap logging	The level and statistics of the log message sent to the syslog server.

The following example displays the outcome of running the **show logging config** command with RFC5424 enabled.

```
FS# show logging
```

```
Syslog logging: enabled
```

```
Console logging: level debugging, 4740 messages logged
```

```
Monitor logging: level debugging, 0 messages logged
```

```
Buffer logging: level debugging, 4745 messages logged
```

```
Statistic log messages: disable
```

```
Statistic log messages to terminal: disable
```

```
Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds
```

```
Count log messages: enable
```

```
Trap logging: level informational, 2641 message lines logged,4155 fail
```

```
logging to 192.168.23.89
```

```
logging to 2000::1
```

```
Delay-send logging: 2641 message lines logged
```

```
logging to 192.168.23.89 by tftp
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to output console and remove terminal
Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
Trap logging	Level of the logs sent to the syslog server and statistics
Delay-send logging	The server address, log sending way and statistics

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.43 show logging count

	Use this command to display the statistics about occurrence times, and the last occurrence time of each module log in the system in privileged mode.	
	show logging count	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	To use the log packet statistics function, run the logging count command in global configuration mode. The show logging count command can show the information of a specific log, occurrence times, and the last occurrence time. You can use the show logging command to check whether the log statistics function is enabled.	
Configuration Examples	The following example displays the result of the show logging count command: <pre>FS# show logging count Module Name Message Name Sev Occur Last Time SYS CONFIG_I 5 1 Jul 6 10:29:57 SYS TOTAL 1</pre>	
Related Commands	Command	Function
	logging count	Enables the log statistics function.
	show logging	Displays basic configuration of log modules and log information in the buffer.
	clear logging	Clears the logs in the buffer.
Platform Description	N/A	

8.44 show logging reverse

	Use this command to display configured parameters and statistics of logs and log messages in the memory buffer at privileged user layer. The log messages are sorted by the timestamp from now to before.	
	show logging reverse	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	N/A												
Command Mode	Privileged EXEC mode												
Usage Guide													
Configuration Examples	The following command displays the result of the show logging reverse command with RFC5424 format disabled. <pre> FS# show logging reverse Syslog logging: enabled Console logging: level debugging, 15495 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 15496 messages logged Standard format: false Timestamp debug messages: datetime Timestamp log messages: datetime Sequence-number log messages: enable Sysname log messages: enable Count log messages: enable Trap logging: level informational, 15242 message lines logged,0 fail logging to 202.101.11.22 logging to 192.168.200.112 Log Buffer (Total 131072 Bytes): have written 1336, 015492: *Sep 19 02:46:28: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up. 015491: *Sep 19 02:46:28: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up. 015490: *Sep 19 02:46:26: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to down. 015489: *Sep 19 02:46:26: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down. 015488: *Sep 19 02:46:13: FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up. 015487: *Sep 19 02:46:13: FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up. </pre> <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Syslog logging</td><td>Logging flag: enabled or disabled</td></tr> <tr> <td>Console logging</td><td>Level of the logs printed on the console, and statistics</td></tr> <tr> <td>Monitor logging</td><td>Level of the logs printed on the VTY window, and statistics</td></tr> <tr> <td>Buffer logging</td><td>Level of the logs recorded in the memory buffer, and statistics.</td></tr> <tr> <td>Standard format</td><td>Standard log format.</td></tr> </table>	Field	Description	Syslog logging	Logging flag: enabled or disabled	Console logging	Level of the logs printed on the console, and statistics	Monitor logging	Level of the logs printed on the VTY window, and statistics	Buffer logging	Level of the logs recorded in the memory buffer, and statistics.	Standard format	Standard log format.
Field	Description												
Syslog logging	Logging flag: enabled or disabled												
Console logging	Level of the logs printed on the console, and statistics												
Monitor logging	Level of the logs printed on the VTY window, and statistics												
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.												
Standard format	Standard log format.												

Timestamp debug messages	Timestamp format of the Debug messages
Timestamp log messages	Timestamp format of the Log messages
Sequence-number log messages	Serial number switch
Sequence log messages	Attaches system names to the logs.
Count log messages	Log statistics function
Trap logging	Level of the logs sent to the syslog server, and statistics
Log Buffer	Log files recorded in the memory buffer

The following example displays the result of the **show logging reverse** command with RFC5424 format enabled.

FS# show logging reverse

Syslog logging: enabled

Console logging: level debugging, 4740 messages logged

Monitor logging: level debugging, 0 messages logged

Buffer logging: level debugging, 4745 messages logged

Statistic log messages: disable

Statistic log messages to terminal: disable

Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10 seconds

Count log messages: enable

Trap logging: level informational, 2641 message lines logged,4155 fail

logging to 192.168.23.89

logging to 2000::1

Delay-send logging: 2641 message lines logged

logging to 192.168.23.89 by tftp

Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292

```
<134>1 2013-07-24T12:29:34.343763Z FS SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881 task="rl_con"
cmd="enable"]
```

```
<134>1 2013-07-24T12:29:33.410123Z FS SYS 6 SHELL_LOGIN [USER@4881 name="" type="" from="console"]
user login success.
```

```
<132>1 2013-07-24T12:20:32.250265Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
```

```
<135>1 2013-07-24T12:20:02.80343Z FS - 7 - - Please config the IP address for capwap.
```

```
<132>1 2013-07-24T12:20:02.80313Z FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
```

```
<135>1 2013-07-24T12:19:33.130290Z FS - 7 - - Please config the IP address for capwap.
```

Field	Description
Syslog logging	Logging flag: enabled or disabled
Console logging	Level of the logs printed on the console, and statistics
Monitor logging	Level of the logs printed on the VTY window, and statistics
Buffer logging	Level of the logs recorded in the memory buffer, and statistics.
Count log messages	Log statistics function
Statistic log messages	Enables/disables log sending periodically
Statistic log messages to terminal	Enables/ disables log sending to console and remote terminal

	Delay-send file name	Local filename of log delay-sending cache, index of write file and delay interval
	Trap logging	Level of the logs sent to the syslog server and statistics
	Delay-send logging	The server address, log sending mode and statistics
	Log Buffer	Log files recorded in the memory buffer
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.45 terminal monitor

	Use this command to show logs on the current VTY window. Use the no form of this command to restore the default setting. terminal monitor terminal no monitor	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Log information is not allowed to be displayed on the VTY window by default.	
Command Mode	Privileged EXEC mode	
Usage Guide	This command only sets the temporary attributes of the current VTY. As the temporary attribute, it is not stored permanently. At the end of the VTY terminal session, the system will use the default setting, and the temporary setting is invalid. This command can be also executed on the console, but it does not take effect.	
Configuration Examples	The following example allows log information to be printed on the current VTY window: FS# terminal monitor	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	
Command History	Version	Description
	N/A	N/A

9 CWMP Commands

9.1 acs password

	Use this command to configure the ACS password to be authenticated for the CPE to connect to the ACS. Use the no form of this command to cancel the configuration.	
	acs password { <i>password</i> <i>encryption-type encrypted-password</i> }	
	no acs password	
Parameter Description	Parameter	Description
	<i>password</i>	Configures the ACS user password to be authenticated for the CPE to connect to the ACS.
	<i>encryption-type</i>	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
	<i>encrypted-password</i>	Specifies the password in encrypted form.
Defaults	encryption-type: 0 encrypted-password: N/A	
Command Mode	CWMP configuration mode	
Usage Guide	Use this command to configure the ACS user password to be authenticated for the CPE to connect to the ACS. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:  The command contains English letters in upper or lower case and numeric characters.  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password. 	
Configuration Examples	The following example configures the ACS password to be authenticated for the CPE to connect to the ACS to 123. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#acs password 123 FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.

	show cwmp status	Displays the running status of CWMP.
	acs username	Configures the ACS username to be authenticated for the CPE to connect to the ACS.
Platform Description	N/A	

9.2 acs url

	Use this command to configure the URL of the ACS to which the CPE will connect. Use the no form of this command to restore the default setting.	
	acs url <i>url</i>	
	no acs url	
Parameter Description	Parameter	Description
	<i>url</i>	Specifies the URL of the ACS.
Defaults	N/A	
Command Mode	CWMP configuration mode	
Usage Guide	Use this command to configure the URL of the ACS to which the CPE will connect. If no ACS URL is manually specified but a dynamic ACS URL is obtained through DHCP, the CPE initiates a connection to the ACS using the dynamically obtained ACS URL. The URL of the ACS should meet the following format requirements: • The URL of the ACS is formatted as http://ip [: port]/ path. • The URL of the ACS consists of at most 255 characters.	
Configuration Examples	The following example specifies the URL of the ACS to http://10.10.10.1: 7547/acs. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#acs url http://10.10.10.1:7547/acs FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform Description	N/A	

9.3 acs username

	Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the no form of this command to restore the default setting.	
	acs username <i>username</i>	
	no acs username	
Parameter Description	Parameter	Description
	<i>username</i>	Configures the ACS username to be authenticated for the CPE to connect to the ACS.
Defaults	N/A	
Command Mode	CWMP configuration mode	
Usage Guide	Configures the ACS username to be authenticated for the CPE to connect to the ACS.	
Configuration Examples	The following example configures the ACS username to be authenticated for the CPE to connect to the ACS to admin. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#acs username admin FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
	acs password	Configures the ACS password to be authenticated for the CPE to connect to the ACS.
Platform Description	N/A	

9.4 cpe back-up

	Use this command to enable the CPE backup function.	
	Use the no form of this command to restore the default setting.	
	cpe back-up [<i>delay-time seconds</i>]	
	no cpe back-up	

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the backup delay time.
Defaults	The default is 60 seconds.	
Command Mode	CWMP configuration mode	
Usage Guide	After upgrading main programs or configurations, CPE cannot communicate with ACS for wrong configuration delivery. Use this command to recover the previous programs and configurations.	
Configuration Examples	The following example disables the CPE backup function. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#no cpe back-up FS(config-cwmp)#</pre>	
Platform Description	N/A	

9.5 cpe inform

	Use this command to configure the periodic notification function of the CPE. Use the no form of this command to restore the default setting	
	cpe inform [<i>interval seconds</i>] [<i>start-time time</i>]	
	no cpe inform	
Parameter Description	Parameter	Description
	<i>seconds</i>	Specifies the periodical notification interval of the CPE in the range from 30 to 3,600 in the unit of seconds.
	<i>time</i>	Specifies the date and time for starting periodical notification in yyyy-mm-ddThh:mm:ss format.
Defaults	The default is 600 seconds.	
Command Mode	CWMP configuration mode	
Usage Guide	Use this command to configure the periodic notification function of the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the	

	periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60 seconds and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60 seconds.  The narrower periodical notification interval allows the ACS to track the latest CPE status more accurately. However, narrower periodical notification interval brings about more sessions between the CPE and the ACS, consuming more resources of them. So the user should specify the periodical notification interval of the CPE to a reasonable value according to the network performance and the ACS performance.	
Configuration Examples	The following example specifies the periodical notification interval of the CPE to 60 seconds. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#cpe inform interval 60 FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform Description	N/A	

9.6 cpe password

	Use this command to configure the CPE password to be authenticated for the ACS to connect to the CPE. Use the no form of this command to cancel the configuration.	
	cpe password { <i>password</i> <i>encryption-type encrypted-password</i> }	
	no cpe password	
Parameter Description	Parameter	Description
	<i>password</i>	Configures the CPE user password to be authenticated for the ACS to connect to the CPE.
	<i>encryption-type</i>	Specifies the encryption type, which can be set to 0 (indicating that no encryption is used) or 7 (indicating that simple encryption is used).
	<i>encrypted-password</i>	Specifies the password in encrypted form.
Defaults	encryption-type: 0 encrypted-password: N/A	

Command Mode	CWMP configuration mode	
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. In general, the encryption type does not need to be specified. The encryption type needs to be specified only when copying and pasting the encrypted password of this command. A valid password should meet the following format requirements:  The command contains English letters and numeric characters.  Blanks are allowed at the beginning of the password but will be ignored. Intermediate and ending blanks, however, are regarded as a part of the password.	
Configuration Examples	The following example configures the CPE password to be authenticated for the ACS to connect to the CPE to 123. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#cpe password 123 FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
	acs username	Configures the CPE username to be authenticated for the ACS to connect to the CPE.
Platform Description	N/A	

9.7 cpe url

	Use this command to configure the URL of the CPE to which the ACS will connect. Use the no form of this command to restore default setting.	
	cpe url <i>url</i>	
	no cpe url	
Parameter Description	Parameter	Description
	<i>url</i>	Specifies the URL of the CPE.
Defaults	N/A	
Command Mode	CWMP configuration mode	

Usage Guide	Use this command to configure the URL of the CPE to which the ACS will connect. If no CPE URL is manually specified but a dynamic CPE URL is obtained through DHCP, the ACS initiates a connection to the CPE using the dynamically obtained CPE URL. The URL of the CPE should meet the following format requirements: ● The URL of the CPE is formatted as http://ip [: port]/ path. ● The URL of the CPE consists of at most 255 characters.	
Configuration Examples	The following example specifies the URL of the CPE to http://10.10.10.1:7547/acs. <pre>FS#configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#cpe url Hhttp://10.10.10.1:7547/ FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform Description	N/A	

9.8 cpe username

	Use this command to configure the ACS username to be authenticated for the CPE to connect to the ACS. Use the no form of this command to restore the default setting.	
	cpe username <i>username</i>	
	no cpe username	
Parameter Description	Parameter	Description
	<i>username</i>	Configures the CPE username to be authenticated for the ACS to connect to the CPE.
Defaults	N/A	
Command Mode	CWMP configuration mode	
Usage Guide	Configures the CPE username to be authenticated for the ACS to connect to the CPE.	
Configuration Examples	The following example configures the CPE username to be authenticated for the ACS to connect to the CPE to admin. <pre>FS#config terminal</pre>	

	Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#cpe username admin FS(config-cwmp)#	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
	cpe password	Configures the CPE password to be authenticated for the ACS to connect to the CPE.
Platform Description	N/A	

9.9 cwmp

	Use this command to enable the CWMP function. Use the no form of this command to disable this function.	
	cwmp	
	no cwmp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults		
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable or disable the CWMP function.	
Configuration Examples	The following example disables the CWMP function. FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#no cwmp FS(config)#	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.

Platform	N/A
Description	

9.10 disable download

	Use this command to disable the function of downloading main program and configuration files from the ACS. Use the no form of this command to restore the default setting.	
	disable download	
	no disable download	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the CPE can download main program and configuration files from the ACS.	
Command Mode	CWMP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example disables the function of downloading main program and configuration files from the ACS. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#disable download FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform Description	N/A	

9.11 disable upload

	Use this command to disable the function of uploading configuration and log files to the ACS. Use the no form of this command to restore the default setting.	
	disable upload	
	no disable upload	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the CPE can upload its configuration and log files to the ACS.	
Command Mode	CWMP configuration mode	
Usage Guide	Disables the function of uploading configuration and log files to the ACS.	
Configuration Examples	The following example disables the function of uploading configuration and log file to the ACS. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#disable upload FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform Description	N/A	

9.12 show cwmp configuration

	Use this command to display the current configuration of CWMP.	
	show cwmp configuration	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privilege EXEC mode	
Usage Guide		
Configuration Examples	The following example displays the current configuration of CWMP. <pre>FS(config-cwmp)#show cwmp configuration</pre>	

```

CWMP Status           : enable
ACS URL               : http://www.FS.com.cn/acs
ACS username          : admin
ACS password          : *****
CPE URL               : http://10.10.10.2:7547/
CPE username          : FS
CPE password          : *****
CPE inform status      : disable
CPE inform interval   : 60s
CPE inform start time : 0:0:0 0 0 0
CPE wait timeout      : 50s
CPE download status    : enable
CPE upload status      : enable
CPE back up status     : enable
CPE back up delay time : 60s
  
```

The descriptions to the fields shown after executing the command **show cwmp configuration**.

Field	Description
CWMP Status	Running status of CWMP.
ACS URL	URL of the ACS.
ACS username	ACS username to be authenticated for the CPE to connect to the ACS.
ACS password	ACS password to be authenticated for the CPE to connect to the ACS.
CPE URL	URL of the CPE.
CPE username	CPE username to be authenticated for the ACS to connect to the CPE.
CPE password	CPE password to be authenticated for the ACS to connect to the CPE.
CPE inform status	Status of CPE periodical notification function.
CPE inform interval	CPE periodical notification interval.
CPE wait timeout	Timeout period of CPE sessions.
CPE inform start time	The start time of periodical notification.
CPE download status	Indicates whether to download main program and configuration files from the ACS.
CPE upload status	Indicates whether to upload configuration files and log files to the ACS.
CPE back up status	Indicates whether backup and restoration of the main program and configuration file is enabled.
CPE back up delay time	Delay time of the backup and restoration of the main program and configuration files.

Related Commands

Command	Description
show cwmp status	Displays the running status of CWMP.

Platform	N/A
Description	

9.13 show cwmp status

	Uses this command to display the running status of CWMP																	
	show cwmp status																	
Parameter Description	Parameter	Description																
	N/A	N/A																
Defaults	N/A																	
Command Mode	Privileged EXEC mode																	
Usage Guide	N/A																	
Configuration Examples	The following example displays the running status of CWMP. <pre>FS#show cwmp status CWMP Status : enable Session status : Close Last success session : Unknown Last success session time : Thu Jan 1 00:00:00 1970 Last fail session : Unknown Last fail session time : Thu Jan 1 00:00:00 1970 Session retry times : 0</pre>																	
	The descriptions to the fields shown after executing the command show cwmp configuration. <table><tr><th>Field</th><th>Description</th></tr><tr><td>CWMP Status</td><td>The running status of CWMP</td></tr><tr><td>Session status</td><td>The current status of the session between the CPE and the ACS</td></tr><tr><td>Last success session</td><td>The last success session type</td></tr><tr><td>Last success session time</td><td>The last success session time</td></tr><tr><td>Last fail session</td><td>The last failed session type</td></tr><tr><td>Last fail session time</td><td>The last failed session time</td></tr><tr><td>Session retry times</td><td>The number of session retransmission attempts</td></tr></table>		Field	Description	CWMP Status	The running status of CWMP	Session status	The current status of the session between the CPE and the ACS	Last success session	The last success session type	Last success session time	The last success session time	Last fail session	The last failed session type	Last fail session time	The last failed session time	Session retry times	The number of session retransmission attempts
Field	Description																	
CWMP Status	The running status of CWMP																	
Session status	The current status of the session between the CPE and the ACS																	
Last success session	The last success session type																	
Last success session time	The last success session time																	
Last fail session	The last failed session type																	
Last fail session time	The last failed session time																	
Session retry times	The number of session retransmission attempts																	
Related Commands	Command	Description																
	show cwmp configuration	Displays the current configuration of CWMP.																

Platform	N/A
Description	

9.14 timer cpe-timeout

	Uses this command to configure the session timeout period of the CPE.	
	timer cpe- timeout <i>seconds</i>	
	no timer cpe-timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the session timeout, in the range from 10 to 600 in the unit of seconds.
Defaults	By default, the session timeout period is 30 seconds.	
Command Mode	CWMP configuration mode	
Usage Guide	Use this command to configure the session timeout period of the CPE. The maximum waiting period that the CPE has when the CPE failed to receive the ACS reply.	
Configuration Examples	The following example configures the session timeout period of the CPE to 50 seconds. <pre>FS#config terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)#cwmp FS(config-cwmp)#timer cpe-timeout 50 FS(config-cwmp)#</pre>	
Related Commands	Command	Description
	show cwmp configuration	Displays the current configuration of CWMP.
	show cwmp status	Displays the running status of CWMP.
Platform	N/A	
Description		

10 Module Hot-plugging/ unplugging Commands

10.1 remove configuration module slot-num

	Use this command to remove the module configurations.	
	remove configuration module <i>slot-num</i>	
Parameter Description	Parameter	Description
	<i>slot-num</i>	Slot number.
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	Use this command to remove the module configurations. This command is invalid for module in on-line status. If there is a module inserted in the slot, this module will be reset.	
Configuration Examples	The following example clears the configuration on slot 4. FS(config)# remove configure module 4	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.2 remove configuration device device-id

	Use this command to remove the configuration on a stacking device, which validates in stacking mode after restart.	
	remove configuration device <i>device-id</i>	
Parameter Description	Parameter	Description
	<i>device-id</i>	The chassis number.
Defaults	N/A	

Command Mode	Global configuration mode	
Usage Guide	This command is used to remove the configuration on a stacking device. It validates after the device is restarted.	
Configuration Examples	The following example clears the configuration on device 1. <pre>FS(config)# remove configuration device 1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.3 show alarm

	Use this command to display system alarm messages, concerning card startup failure, temperature, power, and fan alarms.			
	show alarm			
Parameter Description	Parameter		Description	
	N/A		N/A	
Defaults	N/A			
Command Mode	Privileged EXEC mode			
Usage Guide	N/A			
Configuration Examples	The following example displays system alarm messages.			
	FS#show alarm			
	Dev	Module	Level	Info

	1	DEV	Warning	Some fans are absent.
	1	DEV	Critical	Some cards are in cannot-startup state.
	Field		Description	
	Dev		Device ID	
Module		Service module		
Level		Alarm level, including Critical and Warning		
Info		Alarm cause, such as system power shortage fan absence and card startup failure		

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.4 show manufinfo

	Use this command to display asset information about all independent components in the system for asset management, including the chassis, fan, power, management board, and line card. The information covers the ID, slot number, name, serial number (SN), software and hardware version, and MAC address. Not all devices support display of the same information and only supported information is printed.	
	show manufinfo	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display asset information about all independent components in the system	
Configuration Examples	The following example displays asset information of the single physical device. <pre> FS#show manufinfo Device 1 Location: Chassis Device name: S5860-20SQ Device Serial Number: 62150129A8B0DAF0F0321 Hardware Version: V1.0 Mac Address: 00.D0.F8.00.11.22 Device 2 Location: Power 1 Device name: PSM-C150WAC Device Serial Number: 42150129A8B0DAF0F0322 Hardware Version: V1.0 Device 3 Location: FAN </pre>	

	Device name: AFM-CLR Device Serial Number: 52150129A8B0DAF0F0321 Hardware Version: V1.0	
	The following example displays asset information in stacking mode.	
	FS#show manuinfo Device 1 Location: Chassis 1 Device name: S5860-48SC Device Serial Number: 62150129A8B0DAF0F0321 Hardware Version: V1.0 Mac Address: 00.D0.F8.00.11.22 Device 2 Location: Power 1/1 Device name: PSM-C515WACP Device Serial Number: 42150129A8B0DAF0F0321 Hardware Version: V1.0 Device3 Location: FAN 1 Device name: AFM-CFB Device Serial Number: 52150129A8B0DAF0F0322 Hardware Version: V1.0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.5 show sysmac

	Use this command to display the MAC address of the current system.	
	show sysmac	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode.	

Mode		
Usage Guide	N/A	
Configuration Examples	The following example displays the MAC address of the current system. <pre>FS#show sysmac 00d0.f822.33e2</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10.6 show version module detail

	Use this command to display the details of the module.	
	show version module detail [<i>slot-num</i>] show version module detail [<i>device-id</i> / <i>slot-num</i>]	
Parameter Description	Parameter	Description
	<i>device-id</i>	(Optional) Device ID.
	<i>slot-num</i>	(Optional) Slot ID.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	Use this command to display details of the module	
Configuration Examples	<pre>FS# show version module detail 2 Device : 1 Slot : 2 User Status : none Software Status: none Online Module : Type : Ports : 0 Version : Configured Module : Type :</pre>	

	Ports : Version : FS#	
Related Commands	Command	Description
	show version slots	Displays slot details.
Platform Description	N/A	

10.7 show version slots

	Use this command to display the details of the slot.														
	show version slots [<i>slot-num</i>] show version slots [<i>device-id</i> / <i>slot-num</i>]														
Parameter Description	Parameter	Description													
	<i>slot-num</i>	(Optional) Slot number.													
	<i>device-id</i>	(Optional) Device ID.													
Defaults	N/A														
Command Mode	Privileged EXEC mode.														
Usage Guide	N/A														
Configuration Examples	FS# show version slots <table><thead><tr><th>Dev</th><th>Slot</th><th>Port</th><th>Configured Module</th><th>Online Module</th><th>Software Status</th></tr></thead><tbody><tr><td>1</td><td>0</td><td>32</td><td>S5750C-28GT4XS-H</td><td>S5750C-28GT4XS-H</td><td>master</td></tr></tbody></table>			Dev	Slot	Port	Configured Module	Online Module	Software Status	1	0	32	S5750C-28GT4XS-H	S5750C-28GT4XS-H	master
Dev	Slot	Port	Configured Module	Online Module	Software Status										
1	0	32	S5750C-28GT4XS-H	S5750C-28GT4XS-H	master										
Related Commands	Command	Description													
	show version moduel detail	Displays the details of the module.													
Platform Description	N/A														

11 Supervisor Module Redundancy Commands

11.1 auto-sync time-period

	Use this command to configure the auto-sync time-period of running-config and startup-config when the dual supervisor module is redundant. Use the no form of this command to disable automatic synchronization for the dual supervisor modules. Use the default form of this command to restore the default automatic synchronization time period for the dual supervisor modules.	
	auto-sync time-period <i>value</i>	
	no auto-sync time-period	
	default auto-sync time-period	
Parameter Description	Parameter	Description
	<i>value</i>	Automatic synchronization time interval measured in seconds, in the range from one second to one month (2,678,400 seconds).
Defaults	The default is one hour (3600 seconds) by default.	
Command Mode	Redundancy configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the automatic synchronization interval to 60 seconds. <pre>FS(config)# redundancy FS(config-red)# auto-sync time-period 60 Redundancy auto-sync time-period: enabled (60 seconds). FS(config-red)# exit</pre> The following example disables automatic synchronization. <pre>FS(config)# redundancy FS(config-red)# no auto-sync time-period Redundancy auto-sync time-period: disabled. FS(config-red)# exit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.2 redundancy

	Use this command to enter redundancy configuration mode.	
	redundancy	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enters redundancy configuration mode. <pre>FS# config terminal FS(config)# redundancy FS(config-red)# exit</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.3 redundancy forceswitch

	Use this command to perform active/standby supervisor module switchover.	
	redundancy forceswitch	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If this command is executed on the active supervisor module, the module will be reset and the standby supervisor module will act as an active supervisor module.	

	The following conditions are required to perform hot backup switchover: ● This command is executed on the active supervisor module. There is a standby supervisor module. ● Hot backups on all virtual switch devices (VSDs) are in real-time status. ● Hot backup switchovers on VSDs are not prevented temporarily by any service entity. When there are multiple VSDs, the system judges whether the hot backup on each VSD allows active/standby switchover; If any VSD does not allow the switchover, the command fails. Otherwise, active/standby switchovers are enforced on all VSDs.	
Configuration Examples	The following example performs active/standby supervisor module switchover. <pre>FS# redundancy forceswitch</pre> This operation will reload the master unit and force switchover to the slave unit. Are you sure to continue? [N/y] y	
Related Commands	Command	Description
	reload	Resets the active supervisor module.
Platform Description	N/A	

11.4 redundancy reload

	Use this command to reset the supervisor module.	
	redundancy reload { peer shelf [switchid] }	
Parameter Description	Parameter	Description
	peer	Resets the standby supervisor module.
	shelf	Resets both the active and standby supervisor modules on the device which works as a single physical device. The device ID should be specified on the device which works as a Virtual Switching Unit (stacking) device.
	switchid	stacking device ID, supported on a stacking device.  This parameter is not supported in stand-alone mode. It must be contained in the redundancy reload shelf command in stacking mode.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Resetting the supervisor module does not affect data forwarding. Data forwarding will not be interrupted and the user session information will not be missing. The redundancy reload shelf command is used to reset the device which works as a single physical device. The redundancy reload shelf switchid command is used to reset the specified device which works as a stacking	

	device.	
Configuration Examples	The following example resets the standby supervisor module. <pre>FS# redundancy reload peer</pre> This operation will reload the current slave unit. Are you sure to continue? [N/y] y Preparing to reload peer! The following example resets device 2 which works as a stacking device. <pre>FS# redundancy reload shelf 2</pre> This operation will reload the device 2. Are you sure to continue? [N/y] y Preparing to reload device 2!	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

11.5 show redundancy states

	Use this command to display the current redundancy state.	
	show redundancy states	
Parameter Description	Parameter	Description
	-	-
Defaults	N/A	
Command Mode	User EXEC mode / Privileged EXEC mode	
Usage Guide	Currently, only 1:1 hot backup (for the global active module and standby module) is supported in the stacking mode. Therefore, only the hot backup state of the local and peer device is displayed. If the system is configured with multiple VSDs, the hot backup state of all VSDs is displayed in VSD 0 in global configuration mode.	
Configuration Examples	The following example displays the redundancy states of active supervisor module. <pre>FS> enable FS# show redundancy states Redundancy role: master Redundancy state: realtime Auto-sync time-period: 3600 s</pre>	

Redundancy management role: master

Redundancy control role: active

Redundancy control state: realtime

Auto-sync time-period: 3600 s

The following example displays the redundancy state of the standby supervisor module.

```
FS> enable
```

```
FS# show redundancy states
```

Redundancy role: slave

Redundancy state: realtime

Redundancy management role: slave

Redundancy control role: standby

Redundancy control state: realtime

The following example displays the redundancy state of the candidate supervisor module.

```
FS> enable
```

```
FS# show redundancy states
```

Redundancy role: candidate

Redundancy state: none

Redundancy management role: candidate

Redundancy control role: standby

Redundancy control state: realtime

The following example displays the redundancy state of the active supervisor module with VSD1 and VSD2 configured.

```
FS> enable
```

```
FS# show redundancy states
```

Redundancy role: master

Redundancy state: realtime

Auto-sync time-period: 3600 s

Redundancy management role: master

Redundancy control role: active

Redundancy control state: realtime

Auto-sync time-period: 3600 s

VSD vsd1 redundancy state: realtime

VSD vsd2 redundancy state: realtime

	Field	Description
	role	The role of the supervisor module.
	state	The state of the supervisor module.
	Auto-sync time-period	Displayed on the active supervisor module. The configuration file synchronizes the time interval automatically. "disabled" indicates no automatic synchronization.
	VSD <vsd name> redundancy state	Displays hot backup state of the specified VSD in VSD 0.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

12 Package Management Commands

12.1 show upgrade auto-sync

	Use this command to display related auto-sync configuration on the device. show upgrade auto-sync	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is used to display the auto-sync upgrade configuration in the system including the policy, range and upgrade package's path.	
Prompt Messages	The auto-sync information of the system is displayed after running. <pre>FS#show upgrade auto-sync auto-sync policy: coordinate auto-sync range: vsu auto-sync package: flash:/eg1000m_main_1.0.0.0f328e91.bin</pre>	

12.2 show upgrade file

	Use this command to display the information of the installation package files in the device file system. show upgrade file <i>url</i>	
Parameter Description	Parameter	Description
	<i>url</i>	The local <i>url</i> path indicates where an installation package file is stored.

Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is used to preview main messages of an installation package after it is downloaded into local file system.	
Configuration Examples	The following example displays the information of an installation package file. <pre>FS#\$show flash:S5860_FSOS12.1(1)B0101-FULL_install.bin Name : main Version : 1.0.0.2f1c4dd8 Package type : unknown Size : 166440370 Build time : Fri 23 Nov 2018 09:01:43 UTC Description : main upgrade package Package files : /fdt.img /initrd.img /kernel.img /rboot-S5860.bin</pre>	
Prompt Messages	N/A	

12.3 show upgrade history

	Use this command to display the upgrade history.	
	show upgrade history	
Parameter Description	Parameter	Description
	N/A	N/A

Command Mode	Privileged EXEC mode
Default Level	2
Configuration Examples	The following example displays the upgrade history. <pre> FS#show upgrade history Upgrade History Information: Time : 2018-11-05 06:13:17 Method : OOBTFTP Package Name : S5860.bin Package Type : MAIN Time : 2018-11-06 03:11:16 Method : OOBTFTP Package Name : S5860_FSOS12.1(1)B1_install.bin Package Type : MAIN </pre>
Prompt Messages	N/A
Platforms	N/A

12.4 show upgrade status

	Use this command to display the upgrade status of all line cards on the chassis device. show upgrade status	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode	
Default Level	2	
Configuration Examples	The following example displays the upgrade status of all line cards on the chassis device. <pre> FS#show upgrade status </pre>	

	<pre> [slot: M1] dev_type: s12k-ppc-cm status : ready [slot: 8] dev_type: s12k-s86-ppc-lc status : upgrading </pre>
Prompt Messages	The upgrade status of various line cards is displayed. <pre> [slot: M1] dev_type: s12k-ppc-cm status : ready [slot: 8] dev_type: s12k-s86-ppc-lc status : upgrading </pre>
Platforms	This command is supported only on the chassis device.

12.5 upgrade

	Use this command to install and upgrade an installation package in the local file system. Upgrade <i>url</i> [force]	
Parameter Description	Parameter	Description
	<i>url</i>	The local path indicates where an installation package is stored. This command is used to upgrade an installation package on the device.
	force	Mandatory upgrade
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is applicable to installation packages of all subsystem components, chassis devices, and feature components. Before its use, run the copy command to copy feature packages into the file system in the device. When there is no specified range of parameters, the command is used to upgrade the matched system components according to the auto-sync configuration.	

Configuration Examples	The following example upgrades the main package on the device. <pre> FS#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin Upgrade processing is 10% Upgrade processing is 60% Upgrade processing is 90% Upgrade info [OK] Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f] Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8] Upgrade processing is 100% Reload system to take effect! </pre> The following example upgrades the chassis package on the device. <pre> FS# upgrade usb0:/ S8600E_FSOS11.0(4)B1_CM_install.bin [Slot M1]:Upgrade processing is 10% [Slot 1]:Upgrade processing is 10% [Slot M1]:Upgrade processing is 60% [Slot 1]:Upgrade processing is 60% [Slot M1]:Upgrade processing is 90% [Slot M1]: Upgrade info [OK] Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40] Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085] [Slot M1]:Restart to take effect ! [Slot M1]:Upgrade processing is 100% [Slot 1]:Upgrade processing is 90% [Slot 1]: Upgrade info [OK] Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81] Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8] [Slot 1]:Restart to take effect ! [Slot 1]:Upgrade processing is 100% </pre>

	<pre>[slot: M1] device_name: ca-octeon-cm status: SUCCESS [slot: 1] device_name: ca-octeon-lc Status: SUCCESS</pre>
Verification	Run the show version detail command to check whether the upgrade of a subsystem component is successful. Run the show component command to check whether the upgrade of a feature component is successful. upgrading a feature component
Prompt Messages	The prompt message of successful running is displayed. <pre>Upgrade info [OK]</pre> The installation package is invalid or damaged and needs to be regained for upgrade command. <pre>Invalid package file</pre> The installation package is not available on the device and needs to be regained for upgrade command. <pre>Device don't support</pre> There is no need to upgrade the device. <pre>The version in device is newer or the same</pre> When there is insufficient space for upgrade, check USB flash disk attached on the device. <pre>No enough space for decompress</pre> Contact the service center to solve the system problem. <pre>No enough space,rootfs been destroyed. Please upgrade in uboot</pre>

12.6 upgrade auto

	Use this command to upgrade an installation package automatically without interrupting services on a dual-device stacking system. While either in stacking mode or in standalone mode, one single device will restart after this configuration, thus interrupting services. <pre>upgrade auto url [force]</pre>

Parameter Description	Parameter	Description
	url	Installation package directory
	force	Enforces upgrade.
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	Use this command to upgrade the stacking system. Download the program of the latest version to the device before running this command (by using the copy tftp command). During one upgrade, do not use the upgrade auto command and other upgrade commands (such as the upgrade command) at the same time. If auto-upgrade fails, follow the system prompt to restore the version. Do not update the installation package (by running the copy tftp command/U disk copy) or perform other upgrade operation (running the upgrade /upgrade auto command) repetitively. During auto-upgrade, do not unplug the card, perform hot backup switchover, power off chassis or change stacking software/hardware configuration.	
Configuration Examples	The following example upgrades the main package automatically without interrupting the service. <pre> 2015-04-09_09-56-23 FS#upgrade auto usb0:S5860_FSOS11.0(5)B1_install.bin 2015-04-09_09-56-24 FS#*Jan 1 00:23:40: %7: 2015-04-09_09-56-24 *Jan 1 00:23:40: %7: [Slot 1/0]:Upgrade processing is 10% 2015-04-09_09-56-26 FS#show upgrade status 2015-04-09_09-56-26 [Slot 1/0] 2015-04-09_09-56-26 dev_type: s6k 2015-04-09_09-56-26 status : upgrading 2015-04-09_09-56-26 [Slot 2/0] 2015-04-09_09-56-26 dev_type: s6k 2015-04-09_09-56-26 status : transmission 2015-04-09_09-58-20 *Jan 1 00:25:36: %7: [Slot 2/0]:Upgrade processing is 10% 2015-04-09_09-58-30 FS#show upgrade status 2015-04-09_09-58-30 [Slot 1/0] 2015-04-09_09-58-30 dev_type: s6k 2015-04-09_09-58-30 status : upgrading 2015-04-09_09-58-30 [Slot 2/0] 2015-04-09_09-58-30 dev_type: s6k 2015-04-09_09-58-30 status : upgrading 2015-04-09_09-58-39 *Jan 1 00:25:56: %7: 2015-04-09_09-58-39 *Jan 1 00:25:56: %7: [Slot 2/0]:Upgrade processing is 60% 2015-04-09_09-59-19 *Jan 1 00:26:35: %7: 2015-04-09_09-59-19 *Jan 1 00:26:35: %7: [Slot 2/0]:Upgrade processing is 90% </pre>	

```

2015-04-09_09-59-19 *Jan 1 00:26:35: %7:
2015-04-09_09-59-19 *Jan 1 00:26:35: %7: [Slot 2/0]:
2015-04-09_09-59-19 *Jan 1 00:26:35: %7: Upgrade info [OK]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:   Kernel version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:   Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_09-59-19 *Jan 1 00:26:36: %7:
2015-04-09_09-59-19 *Jan 1 00:26:36: %7: [Slot 2/0]:Reload system to take effect!
2015-04-09_09-59-21 *Jan 1 00:26:37: %7:
2015-04-09_09-59-21 *Jan 1 00:26:37: %7: [Slot 2/0]:Upgrade processing is 100%
2015-04-09_10-00-28 FS#show upgrade status
2015-04-09_10-00-28 [Slot 1/0]
2015-04-09_10-00-28      dev_type: s6k
2015-04-09_10-00-28      status  : upgrading
2015-04-09_10-00-28 [Slot 2/0]
2015-04-09_10-00-28      dev_type: s6k
2015-04-09_10-00-28      status  : success
2015-04-09_10-01-39 *Jan 1 00:28:56: %7:
2015-04-09_10-01-39 *Jan 1 00:28:56: %7: [Slot 1/0]:Upgrade processing is 60%
2015-04-09_10-02-17 *Jan 1 00:29:33: %7:
2015-04-09_10-02-17 *Jan 1 00:29:33: %7: [Slot 1/0]:Upgrade processing is 90%
2015-04-09_10-02-17 *Jan 1 00:29:33: %7:
2015-04-09_10-02-17 *Jan 1 00:29:33: %7: [Slot 1/0]:
2015-04-09_10-02-17 *Jan 1 00:29:34: %7: Upgrade info [OK]
2015-04-09_10-02-17 *Jan 1 00:29:34: %7:   Kernel version[2.6.32.6b311610a8eb91->2.6.32.6b31161115502c]
2015-04-09_10-02-17 *Jan 1 00:29:34: %7:   Rootfs version[1.0.0.eb75cd01->1.0.0.3d978b6c]
2015-04-09_10-02-17 *Jan 1 00:29:34: %7:
2015-04-09_10-02-18 *Jan 1 00:29:34: %7: [Slot 1/0]:Reload system to take effect!
2015-04-09_10-02-19 *Jan 1 00:29:35: %7:
2015-04-09_10-02-19 *Jan 1 00:29:35: %7: [Slot 1/0]:Upgrade processing is 100%
2015-04-09_10-02-19 *Jan 1 00:29:36: %7: %PKG_MGMT:auto-sync config synchronization, Please wait for a
moment....
2015-04-09_10-02-20 *Jan 1 00:29:36: %7:
2015-04-09_10-02-20 [ 1784.116069] rtc-pcf8563 6-0051: retrieved date/time is not valid.
2015-04-09_10-02-20 *Jan 1 00:29:36: %7: [Slot 2/0]:auto sync config: space not enough left 57229312, need
114597815
2015-04-09_10-02-20 *Jan 1 00:29:36: %7:
2015-04-09_10-02-20 *Jan 1 00:29:36: %7: [Slot 2/0]:auto sync package config err
2015-04-09_10-02-20 *Jan 1 00:29:37: %7: [Slot 1/0]
2015-04-09_10-02-21 *Jan 1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan 1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan 1 00:29:37: %7: [Slot 2/0]
2015-04-09_10-02-21 *Jan 1 00:29:37: %7:   device_name: s6k
2015-04-09_10-02-21 *Jan 1 00:29:37: %7:   status:      SUCCESS
2015-04-09_10-02-21 *Jan 1 00:29:38: %7: %Do with dtm callback....

```

```
2015-04-09_10-02-21 *Jan  1 00:29:38: %vsu-5-DTM_AUTO_UPGRADE: Upgrading the system, wait a moment please.
```

12.7 upgrade auto-sync package

	Use this command to configure the path for the auto-sync upgrade.	
	upgrade auto-sync package <i>url</i>	
Parameter Description	Parameter	Description
	<i>url</i>	The path of installation package.
Defaults	The default is the last upgrade path.	
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	It is recommended to use default settings.	
Configuration Examples	The following example sets the path to the upgrade package in the USB flash disk. <pre>FS# upgrade auto-sync package usb0:/eg1000m_main_1.0.0.0f328e91.bin</pre>	
Verification	Run the show upgrade auto-sync command to display current auto-sync policy. If <i>url</i> provides normal path, run the stat command to check whether it can be accessed.	
Prompt Messages	The prompt message of successful running is displayed: Upgrade auto-sync package is set as usb0:/eg1000m_main_1.0.0.0f328e91.bin	

12.8 Upgrade auto-sync policy

	Use this command to set an auto-sync policy for the system. upgrade auto-sync policy [none compatible coordinate]	
Parameter Description	Parameter	Description
	none	No auto-sync upgrade
	compatible	Performs auto-synchronization based on the sequential order of versions.
	coordinate	Synchronizes with the version based on the system upgrade patch stored on the supervisor module.
Defaults	coordinate	
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	Check whether the upgrade package is ready before using the command.	
Configuration Examples	The following example sets the auto-sync policy of the device based on the version of supervisor modules. <pre>FS# upgrade auto-sync policy coordinate</pre>	
Verification	Display the current policy for auto-sync upgrade by running the show upgrade auto-sync command.	
Prompt Messages	The prompt message of successful running is displayed. <pre>Upgrade auto-sync policy is set as coordinate.</pre>	

12.9 upgrade auto-sync range

	Use this command to set the range of auto-sync upgrade. upgrade auto-sync range [chassis vsu]	
Parameter Description	Parameter	Description
	chassis	Auto-sync version upgrade in the range of chassis
	Vsu	Auto-sync version upgrade in the range of the vsu system.
Defaults	Vsu	
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	It is recommended to set the parameter to stacking to ensure system version consistency to the most extent.	
Configuration Examples	The following example installs the auto-sync upgrade in the stacking system. <pre>FS# upgrade auto-sync range vsu</pre>	
Verification	Run the show upgrade auto-sync command to display the range of current auto-sync upgrade.	
Prompt Messages	The prompt message of successful running is displayed. <pre>Upgrade auto-sync range is set as vsu</pre>	

12.10 upgrade download tftp

	Use this command to download, install and upgrade installation packages from the tftp server. upgrade download tftp://path [vrf vrf-name] [force] upgrade download oob_tftp://path [via mgmt {number}] [force]

Parameter Description	Parameter	Description
	<i>path</i>	The path of installation packages on the tftp server This command is downloaded and upgraded automatically from the server.
	vrf <i>vrf-name</i>	Specifies a VRF for downloading the installation package.
	via <i>mgmt number</i>	If the transfer mode is <i>oob_tftp</i> and there are multiple MGMT ports, you can select a specific port.
	force	Enforces upgrade.
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is applicable to installation packages of all subsystem components and chassis devices. This command is used to perform automatic installation, copy and upgrade of files.	
Configuration Examples	The following example upgrades the device. <pre> FS#upgrade download tftp://172.30.31.176/S5860_FSOS12.1(1)B0101-FULL_install.bin *Nov 23 13:21:38: %UPGRADE-6-INFO: Start upgrade *Nov 23 13:21:39: %UPGRADE-6-INFO: Copy to /tmp/vsd/0/upgrade_rep/ *Nov 23 13:21:39: %UPGRADE-6-INFO: Please wait for a moment..... Press Ctrl+C to quit !! !! FS#*Nov 16 19:09:00: %UPGRADE-6-INFO: Upgrade disable reload device *Nov 16 19:09:00: %UPGRADE-6-INFO: Upgrade disable redundancy forceswitch *Nov 16 19:09:00: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 10% *Nov 16 19:09:03: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 30% *Nov 16 19:09:05: %UPGRADE-6-INFO: (*2/0) Upgrade get package from master device, wait a moment..... *Nov 16 19:11:23: %UPGRADE-6-INFO: (*2/0) Upgrade check package md5 value, wait a moment *Nov 16 19:11:34: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 60% *Nov 16 19:11:35: %UPGRADE-6-INFO: Upgrade processing is 10% *Nov 16 19:11:37: %UPGRADE-6-INFO: Upgrade processing is 30%</pre>	

	<pre>*Nov 16 19:11:39: %UPGRADE-6-INFO: Upgrade check package md5 value, wait a moment *Nov 16 19:11:41: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK] *Nov 16 19:11:41: %UPGRADE-6-INFO: (*2/0) Rootfs version[1.0.0.aca71d43->1.0.0.aca71d43] *Nov 16 19:11:41: %UPGRADE-6-INFO: (*2/0) Reload system to take effect ! *Nov 16 19:11:50: %UPGRADE-6-INFO: Upgrade processing is 60% *Nov 16 19:12:40: %UPGRADE-6-INFO: Upgrade info [OK] *Nov 16 19:12:40: %UPGRADE-6-INFO: Rootfs version[1.0.0.aca71d43->1.0.0.aca71d43] *Nov 16 19:12:40: %UPGRADE-6-INFO: Reload system to take effect ! *Nov 16 19:13:20: %UPGRADE-6-INFO: Upgrade enable redundancy forceswitch *Nov 16 19:13:20: %UPGRADE-6-INFO: Upgrade enable reload device *Nov 16 19:13:20: %UPGRADE-6-INFO: Upgrade processing is 100% *Nov 16 19:13:20: %UPGRADE-6-INFO: Upgrade finish</pre>
Verification	Run the show version command to check whether the upgrade of a feature component is successful.
Prompt Messages	The prompt message of successful running is displayed. <pre>Upgrade info [OK];</pre> The installation package is invalid or damaged and needs to be regained for upgrade command. <pre>Invalid package file</pre> The installation package is not available on the device and needs to be regained for upgrade command. <pre>Device don't support</pre> There is no need to upgrade the device. <pre>The version in device is same</pre> When there is insufficient space for upgrade, check USB flash disk attached on the device. <pre>No enough space for decompress</pre>

12.11 upgrade download ftp

	Use this command to download, install and upgrade installation packages from the ftp server. <pre>upgrade download ftp://path [vrf vrf-name] [force]</pre> <pre>upgrade download oob_ftp://path [via mgmt {number}] [force]</pre>

Parameter Description	Parameter	Description
	<i>path</i>	The path of installation packages on the ftp server This command is downloaded and upgraded automatically from the server.
	vrf <i>vrf-name</i>	Specifies a VRF for downloading the installation package.
	via <i>mgmt number</i>	If the transfer mode is <i>oob_tftp</i> and there are multiple MGMT ports, you can select a specific port.
	force	Enforces upgrade.
Command Mode	Privileged EXEC mode	
Default Level	2	
Usage Guide	This command is applicable to installation packages of all subsystem components and chassis devices. This command is used to perform automatic installation, copy and upgrade of files.	
Configuration Examples	The following example upgrades the device. <pre> FS#upgrade download ftp://user:123456@172.30.31.176/S5860_FSOS12.1(1)B1_install-11-15.bin *Nov 16 18:55:00: %UPGRADE-6-INFO: Start upgrade *Nov 16 18:55:01: %UPGRADE-6-INFO: Copy to /data/upgrade_rep/ *Nov 16 18:55:01: %UPGRADE-6-INFO: Please wait for a moment..... temp_patch_file = /data/upgrade_rep/_temp_S5860_FSOS12.1(1)B1_install-11-15.bin_ Press Ctrl+C to quit ===== >100% *Nov 16 18:59:37: %UPGRADE-6-INFO: Upgrade disable reload device *Nov 16 18:59:37: %UPGRADE-6-INFO: Upgrade disable redundancy forceswitch *Nov 16 18:59:37: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 10% FS#*Nov 16 18:59:39: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 30% *Nov 16 18:59:43: %UPGRADE-6-INFO: (*2/0) Upgrade get package from master device, wait a moment..... *Nov 16 19:01:54: %UPGRADE-6-INFO: (*2/0) Upgrade check package md5 value, wait a moment *Nov 16 19:02:04: %UPGRADE-6-INFO: (*2/0) Upgrade processing is 60%</pre>	

	<pre> *Nov 16 19:02:06: %UPGRADE-6-INFO: Upgrade processing is 10% *Nov 16 19:02:08: %UPGRADE-6-INFO: Upgrade processing is 30% *Nov 16 19:02:10: %UPGRADE-6-INFO: Upgrade check package md5 value, wait a moment *Nov 16 19:02:12: %UPGRADE-6-INFO: (*2/0) Upgrade info [OK] *Nov 16 19:02:12: %UPGRADE-6-INFO: (*2/0) Rootfs version[1.0.0.aca71d43->1.0.0.aca71d43] *Nov 16 19:02:12: %UPGRADE-6-INFO: (*2/0) Reload system to take effect ! *Nov 16 19:02:21: %UPGRADE-6-INFO: Upgrade processing is 60% *Nov 16 19:02:31: %UPGRADE-6-INFO: Upgrade info [OK] *Nov 16 19:02:31: %UPGRADE-6-INFO: Rootfs version[1.0.0.aca71d43->1.0.0.aca71d43] *Nov 16 19:02:31: %UPGRADE-6-INFO: Reload system to take effect ! *Nov 16 19:02:32: %UPGRADE-6-INFO: Upgrade enable redundancy forceswitch *Nov 16 19:02:32: %UPGRADE-6-INFO: Upgrade enable reload device *Nov 16 19:02:32: %UPGRADE-6-INFO: Upgrade processing is 100% *Nov 16 19:02:32: %UPGRADE-6-INFO: Upgrade finish </pre>
Verification	Run the show version detail command to check whether the upgrade of a subsystem component is successful. Run the show component command to check whether the upgrade of a feature component is successful.
Prompt Messages	The prompt message of successful running is displayed. <pre>Upgrade info [OK];</pre> The installation package is invalid or damaged and needs to be regained for upgrade command. <pre>Invalid package file</pre> The installation package is not available on the device and needs to be regained for upgrade command. <pre>Device don't support</pre> There is no need to upgrade the device. <pre>The version in device is same</pre> When there is insufficient space for upgrade, check USB flash disk attached on the device. <pre>No enough space for decompress</pre>

13 OpenFlow Commands

13.1 of controller-ip

	Use this command to enable OpenFlow. of controller-ip <i>ip-address</i> [port <i>port-id</i>] [aux] interface <i>interface-id</i>]	
	Use the no form of this command to disable OpenFlow. no of controller-ip [<i>ip-address</i>]	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Controller IP address. If you configure the no form of this command without any parameter, all controllers are disabled. (OpenFlow1.3 supports connection to multiple controllers and OpenFlow1.0 supports connection to one single controller).
	port <i>port-id</i>	Controller access port ID. The default for OpenFlow1.0 is 6633 and for OpenFlow1.3 is 6653.
	aux	Auxiliary switch (it takes effect for only OpenFlow1.3)
	Interface <i>interface-id</i>	Interface ID, whether out-of-band MGMT interface or in-band physical port (some devices may not have MGMT interfaces).
Command Mode	Global configuration mode	
Default	OpenFlow is disabled by default.	
Usage Guide	N/A	
Configuration Examples	The following example enables OpenFlow. <pre>FS(config)#of controller-ip 192.168.21.57 interface gigabitEthernet 0/1</pre> The following example disables OpenFlow. <pre>FS#no of controller-ip</pre>	

13.2 of mode

	Use this command to configure the controller mode. of mode [single multiple] Use the no form of this command to restore the default setting. no of mode	
Parameter Description	Parameter	Description
	N/A	N/A
Command	Global configuration mode	

Mode	
Default	The default mode is multiple.
Usage Guide	Configure this command before enabling the controller.
Configuration Examples	The following example enables the single mode. <pre>FS(config)#of mode single</pre> The following example enables the multiple mode. <pre>FS(config)#of mode multiple</pre> The following example restores the default setting. <pre>FS(config)#no of mode</pre>

13.3 of packet table-lookup

	Use this command to enable table-lookup mode or disable table-lookup mode. of packet table-lookup [enable disable] no of packet table-lookup	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	The table-lookup mode is enabled by default.	
Usage Guide	N/A	
Configuration Examples	The following example enables the table-lookup mode. <pre>FS(config)#of packet table-lookup enable</pre> The following example disables the table-lookup mode. <pre>FS(config)#of packet table-lookup disable</pre> The following example restores the default setting. <pre>FS(config)#no of packet table-lookup</pre>	

13.4 of packet vlantag

	Use this command to determine whether to contain the VLAN tag in the packet sent by the OpenFlow device. [no] of packet vlantag	
Parameter Description	Parameter	Description
	N/A	N/A
Command	Global configuration mode	

Mode	
Default	The VLAN tag is contained in the packet sent by the OpenFlow device by default.
Usage Guide	N/A
Configuration Examples	The following example contains the VLAN tag in the packet sent by the OpenFlow device. <pre>FS(config)#of packet vlantag</pre> The following example does not contain the VLAN tag in the packet sent by the OpenFlow device.. <pre>FS(config)#no of packet vlantag</pre>

13.5 show of

	Use this command to display the connection between the current device and the controller. show of	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	Use this command to display the OpenFlow version on the device.	
Configuration Examples	The following example displays the connection between the current device and the controller. <pre>FS#show of</pre>	

13.6 show of flowtable

	Use this command to display flow table entries of OpenFlow Device show of flowtable	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	Running the of controller-ip command before configuring this command. Otherwise, the flow table entries are not displayed.	

Configuration	The following example display flow table entries.
Examples	FS#show of flowtable

13.7 show of group

	Use this command to display group information of OpenFlow device. show of group	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	This command takes effect only for OpenFlow1.3.	
Configuration Examples	The following example displays group information of OpenFlow device. FS(config)#show of group	

13.8 show of mergedflow

	Use this command to display merged entries of OpenFlow device. show of mergedflow	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	This command takes effect only for OpenFlow1.3. See the show of flowtable command for parameter description.	
Configuration Examples	The following example displays merged entries of OpenFlow device. FS(config)#show of mergedflow	

13.9 show of meter

	Use this command to display meter information of OpenFlow device. show of meter	
Parameter Description	Parameter	Description
	N/A	N/A
Command	Global configuration mode	

Mode	
Default	N/A
Usage Guide	This command takes effect only for OpenFlow1.3.
Configuration Examples	The following example displays meter information of OpenFlow device. <pre>FS(config)#show of meter</pre>

13.10 show of port

	Use this command to display port information of OpenFlow device. show of port	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	Running the of controller-ip command before configuring this command. Otherwise, the port information is not displayed.	
Configuration Examples	The following example displays port information of OpenFlow device. <pre>FS#show of port</pre>	

13.11 show of mergedflow

	Use this command to display merged flow information. show of mergedflow	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode	
Default	N/A	
Usage Guide	This command is active only for OpenFlow1.3.	
Configuration Examples	The following example displays merged flow information. <pre>FS(config)#show of mergedflow</pre>	

ACL & QoS Configuration Commands

1 ACL Commands

1.1 Command ID Table

For IDs used in the following commands, refer to the command ID table below:

ID	Meaning
ID	Number of access list. Range: Standard IP ACL: 1 to 99, 1300 to 1999 Extended IP ACL: 100 to 199, 2000 to 2699 Extended MAC ACL: 700 to 799 Extended expert ACL: 2700 to 2899
name	ACL name
sn	ACL SN (products can be set according to the priority)
start-sn	Start sequence number
inc-sn	Sequence number increment
deny	If matched, access is denied.
permit	If matched, access is permitted.
port	Protocol number. For IPv6, this field can be IPv6, ICMP, TCP, UDP and numbers 0 to 255. For IPv4, it can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, AHP, ESP, PCP, PIM and IP, or it can be numbers 0 to 255 that represent the IP protocol. It is described when some important protocols, such as ICMP, TCP and UDP, are listed individually.
interface idx	Interface index
src	Packet source IP address (host address or network address)
src-wildcard	Source IP address wildcard. It can be discontinuous, for example, 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type
dst-ipv6-pfix	Destination IPv6 network address or network type
pfix-len	Prefix mask length
src-ipv6-addr	Source IPv6 address
dst-ipv6-addr	Destination IPv6 address
dscp	Differential service code point, and code point value. Range: 0 to 63
flow-label	Flow label in the range 0 to 1048575
dst	Packet destination IP address (host address or network address)
dst-wildcard	Destination IP address wildcard. It can be discontinuous, such as 0.255.0.32
fragment	Packet fragment filtering.

precedence	Packet precedence value (0 to 7)
range	The layer 4 port number range of the packet.
time-range tm-rng-name	Time range of packet filtering, named <i>tm-rng-name</i>
tos	Type of service (0 to 15)
cos	Class of service (0-7)
cos inner cos	COS of the packet tag
icmp-type	ICMP message type (0 to 255)
icmp-code	ICMP message type code (0 to 255)
icmp-message	ICMP message type name (0 to 255)
operator port[port]	Operator (lt-smaller, eq-equal, gt-greater, neq-unequal, range-range) <i>port</i> indicates the port number. Dyadic operation needs two port numbers, while other operators only need one port number
src-mac-addr	Physical address of the source host
dst-mac-addr	Physical address of the destination host
VID vid	VLAN ID
VID inner vid	VID of the tag
ethernet-type	Ethernet protocol type. 0x value can be entered.
match-all tcpf	Match all bits of the TCP flag.
established	Match the RST or ACK bit of the TCP flag.
text	Remark text
in	Filter the incoming packets of the interface
out	Filter the outgoing packets of the interface
{rule mask offset}⁺	rule: Hexadecimal value field; mask: Hexadecimal mask field offset: Refer to the offset table “+” sign indicates at least one group
log	Output the matching syslog when the packet matches the ACL rule.

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol number	35
C	Data frame length field	12	Q	IP check sum	36
D	VLAN tag field	14	R	Source IP address	38
E	DSAP (Destination Service Access Point) field	18	S	Destination IP address	42
F	SSAP (Source Service Access Point) field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48

H	Org Code field	21	V	Sequence number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version number	26	XY	IP header length and reserved bits	58
K	TOS field	27	Z	Resrved bits and flags bit	59
L	Length of IP packet	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

1.2 access-list

	Use this command to create an access list to filter data packets. Use the no form of this command to remove the specified access list.
	Standard IP access list (1 to 99, 1300 to 1999)
	access-list <i>id</i> { deny permit } { <i>source source-wildcard</i> host <i>source</i> any interface <i>idx</i> } [time-range <i>tm-range-name</i>] [log]
	Extended IP access list (100 to 199, 2000 to 2699)
	access-list <i>id</i> { deny permit } protocol { <i>source source-wildcard</i> host <i>source</i> any interface <i>idx</i> } { <i>destination destination-wildcard</i> host <i>destination</i> any } [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [range <i>lower upper</i>] [time-range <i>time-range-name</i>] [log]
	Extended MAC access list (700 to 799)
	access-list <i>id</i> { deny permit } { any host <i>source-mac-address</i> <i>source-mac-address mask</i> } { any host <i>destination-mac-address</i> <i>destination-mac-address mask</i> } [ethernet-type][cos [<i>out</i>][<i>inner in</i>]]
	Extended expert access list (2700 to 2899)
	access-list <i>id</i> { deny permit } [protocol [ethernet-type][cos [<i>out</i>][<i>inner in</i>]]] [VID [<i>out</i>][<i>inner in</i>]] { source <i>source-wildcard</i> host <i>source</i> any } { host <i>source-mac-address</i> any } { destination <i>destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any } [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [time-range <i>time-range-name</i>]
	When you select the Ethernet-type field or cos field:
	access-list <i>id</i> { deny permit } [ethernet-type cos [<i>out</i>][<i>inner in</i>]]] [VID [<i>out</i>][<i>inner in</i>]] { source <i>source-wildcard</i> host <i>source</i> any } { host <i>source-mac-address</i> any } { destination <i>destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any } [time-range <i>time-range-name</i>]
	When you select the protocol field:
	access-list <i>id</i> { deny permit } protocol [VID [<i>out</i>][<i>inner in</i>]]] { source <i>source-wildcard</i> host <i>source</i> any } { host <i>source-mac-address</i> any } { destination <i>destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any } [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [range <i>lower upper</i>] [time-range <i>time-range-name</i>]
	Extended expert ACLs of some important protocols:
	Internet Control Message Protocol (ICMP)
	access-list <i>id</i> { deny permit } icmp [VID [<i>out</i>][<i>inner in</i>]]] { source <i>source-wildcard</i> host <i>source</i> any } { host <i>source-mac-address</i> any } { destination <i>destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any } [<i>icmp-type</i>] [[<i>icmp-type</i> <i>icmp-code</i>]] [<i>icmp-message</i>]] [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [time-range <i>time-range-name</i>]
	Transmission Control Protocol (TCP)

	access-list <i>id</i> { deny permit } tcp [VID [<i>out</i>][<i>inner in</i>]]{ source <i>source-wildcard</i> host <i>Source</i> any } { host <i>source-mac-address</i> any }] { destination <i>destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any }] [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragment] [range <i>lower upper</i>] [time-range <i>time-range-name</i>] [match-all <i>tcp-flag</i> established]	
	User Datagram Protocol (UDP)	
	access-list <i>id</i> { deny permit } udp [VID [<i>out</i>] [<i>inner in</i>]] { <i>source source-wildcard</i> host <i>source</i> any } { host <i>source-mac-address</i> any }] { <i>destination destination-wildcard</i> host <i>destination</i> any } { host <i>destination-mac-address</i> any } [[precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>]] [fragment] [range <i>lower upper</i>][time-range <i>time-range-name</i>]	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number. The ranges available are 1 to 99, 100 to 199, 1300 to 1999, 2000 to 2699, 2700 to 2899, and 700 to 799.
	<i>deny</i>	If not matched, access is denied.
	<i>permit</i>	If matched, access is permitted.
	<i>source</i>	Specify the source IP address (host address or network address).
	<i>source-wildcard</i>	It can be discontinuous, for example, 0.255.0.32.
	<i>protocol</i>	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
	<i>destination</i>	Specify the destination IP address (host address or network address).
	<i>destination-wildcard</i>	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
	<i>fragment</i>	Packet fragment filtering
	<i>precedence</i>	Specify the packet priority.
	<i>precedence</i>	Packet precedence value (0 to 7)
	<i>range</i>	Layer4 port number range of the packet.
	<i>lower</i>	Lower limit of the layer4 port number.
	<i>upper</i>	Upper limit of the layer4 port number.
	<i>time-range</i>	Time range of packet filtering
	<i>time-range-name</i>	Time range name of packet filtering
	<i>tos</i>	Specify type of service.
	<i>tos</i>	ToS value (0 to 15)
	<i>dscp</i>	Differentiated service code point
	<i>dscp</i>	Code point value, ranging from 0 to 63
	<i>icmp-type</i>	ICMP message type (0 to 255)
	<i>icmp-code</i>	ICMP message type code (0 to 255)
	<i>icmp-message</i>	ICMP message type name
	<i>host source-mac-address</i>	Source physical address
	<i>host destination-mac-address</i>	Destination physical address
	<i>VID vid</i>	Match the specified VID.

	<i>ethernet-type</i>	Ethernet type
	match-all	Match all the bits of the TCP flag.
	<i>tcp-flag</i>	Match the TCP flag.
	established	Match the RST or ACK bits, not other bits of the TCP flag.
Defaults	N/A	
Command Mode	Global configuration mode.	
Usage Guide	To filter the data by using the access control list, you must first define a series of rule statements by using the access list. You can use ACLs of the appropriate types according to the security needs: The standard IP ACL (1 to 99, 1300 to 1999) only controls the source IP addresses. The extended IP ACL (100 to 199, 2000 to 2699) can enforce strict control over the source and destination IP addresses. The extended MAC ACL (700 to 799) can match against the source/destination MAC addresses and Ethernet type. The extended expert access list (2700 to 2899) is a combination of the above and can match and filter the VLAN ID. For the layer-3 routing protocols including the unicast routing protocol and multicast routing protocol, the following parameters are not supported by the ACL: precedence <i>precedence/tos tos/fragments/range lower upper/time-range time-range-name</i> The TCP Flag includes part or all of the following: ● urg ● ack ● psh ● rst ● syn ● fin The packet precedence is as below: ● critical ● flash ● flash-override ● immediate ● internet ● network ● priority ● routine The service types are as below: ● max-reliability ● max-throughput ● min-delay ● min-monetary-cost	

- normal

The ICMP message types are as below:

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- device-advertisement
- device-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

The TCP ports are as follows. A port can be specified by port name and port number:

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- ldg
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The UDP ports are as follows. A UDP port can be specified by port name and port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo

- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

The Ethernet types are as below:

- aarp
- appletalk
- decnet-iv
- diagnostic
- etype-6000
- etype-8042
- lat
- lavc-sca
- mop-console
- mop-dump
- mumps
- netbios
- vines-echo
- xns-idp

The UDF headers are as below:

- l2-head
- l3-head
- l4-head
- l5-head

Run **no {sn | permit | deny}** in ACL mode to delete ACEs.

Configuration	1. Example of the standard IP ACL
Examples	The following basic IP ACL allows the packets whose source IP addresses are 192.168.1.64 - 192.168.1.127 to pass:

<pre>FS (config)#access-list 1 permit 192.168.1.64 0.0.0.63</pre> 2. Example of the extended IP ACL The following extended IP ACL allows the DNS messages and ICMP messages to pass: <pre>FS(config)#access-list 102 permit tcp any any eq domain log FS(config)#access-list 102 permit udp any any eq domain log FS(config)#access-list 102 permit icmp any any echo log FS(config)#access-list 102 permit icmp any any echo-reply</pre> 3. Example of the extended MAC ACL This example shows how to deny the host with the MAC address 00d0f8000c0c to provide service with the protocol type 100 on gigabit Ethernet port 1/1. The configuration procedure is as below: <pre>FS(config)#access-list 702 deny host 00d0f8000c0c any aarp FS(config)# interface gigabitethernet 1/1 FS(config-if)# mac access-group 702 in</pre> 4. Example of the extended expert ACL The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.12.3 and the source MAC address 00d0.f800.0044. <pre>FS(config)#access-list 2702 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any FS(config)# access-list 2702 permit any any any any FS(config)# show access-lists expert access-list extended 2702 10 deny tcp host 192.168.12.3 mac 00d0.f800.0044 any any 10 permit any any any any</pre>		
Related Commands	Command	Description
	show access-lists	Show all the ACLs.
	mac access-group	Apply the extended MAC ACL on the interface.
Platform Description	N/A	

1.3 access-list list-remark

Use this command to write a helpful comment (remark) for an access list. Use the no form of this command to remove the remark.		
access-list id list-remark text		
no access-list id list-remark		
Parameter Description	Parameter	Description
	id	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199, 2000 to 2699. Extended MAC ACL: 700 to 799.

		Extended Expert ACL: 2700 to 2899.
	<i>text</i>	Comment that describes the access list.
Defaults	The access lists have no remarks by default.	
Command Mode	Global configuration mode	
Usage Guide	You can use this command to write a helpful comment for a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access list.	
Configuration Examples	The following example writes a comment of "this acl is to filter the host 192.168.4.12" for ACL100. <pre>FS(config)# ip access-list extended 100 FS(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12</pre>	
Related Commands	Command	Description
	show access- lists	Displays all access lists, including the remarks for the access lists.
	show access-lists <i>id</i>	Displays the access list of a specified number, including the remarks for the access list.
	show access-lists <i>name</i>	Displays the access list of a specified name, including the remarks for the access list.
Platform Description		

1.4 access-list remark

	Use this command to write a helpful comment (remark) for an entry in a numbered access list. Use the no form of this command to remove the remark.	
	access-list <i>id</i> remark <i>text</i>	
	no access-list <i>id</i> remark <i>text</i>	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number. Standard IP ACL: 1 to 99, 1300 to 1999. Extended IP ACL: 100 to 199, 2000 to 2699. Extended MAC ACL: 700 to 799. Extended Expert ACL: 2700 to 2899.
	<i>text</i>	Comment that describes the access list entry.
Defaults	The access list entries have no remarks by default.	

Command Mode	Global configuration mode	
Usage Guide	You can use this command to write a helpful comment for an entry in a specified access list. If the specified access list does not exist, the command will create the access list, then add remarks for the access entry.	
Configuration Examples	The following example writes a comment for an entry in ACL102. <pre>FS(config)# access-list 102 remark deny-host-10.1.1.1</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists, including the remarks for the access list entries.
	show access-lists <i>id</i>	Displays the access list of a specified number, including the remarks for the access list entry.
	show access-lists <i>name</i>	Displays the access list of a specified name, including the remarks for the access list entry.
Platform Description		

1.5 clear counters access-list

	Use this command to clear counters of packets matching ACLs.	
	clear counters access-list [<i>id</i> <i>name</i>]	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number
	<i>name</i>	Access list name
Defaults		
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the counters of packets matching the specified or all ACLs.	
Configuration Examples	The following example clears the packet matching counter of ACL No. 2700: <pre>FS #show access-lists 2700 expert access-list extended 2700 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (88 matches) 20 deny tcp any any eq login any any (33455 matches)</pre>	

	<pre> 30 permit tcp any any host 192.168.6.9 any (10 matches) FS# clear counters access-list 2700 FS #show access-lists 2700 expert access-list extended 2700 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any 20 deny tcp any any eq login any any 30 permit tcp any any host 192.168.6.9 any </pre>	
Related Commands	Command	Description
	expert access-list	Defines an expert ACL.
	deny	Defines a deny ACL entry.
	permit	Defines a permits ACL entry.
Platform Description	N/A	

1.6 clear access-list counters

	Use this command to clear counters of packets matching the deny entries in ACLs.	
	clear access-list counters [<i>id</i> <i>name</i>]	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number
	<i>name</i>	Access list name
Defaults		
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the counters of packets matching the deny entries in ACLs.	
Configuration Examples	The following example clears the packet matching counter of ACL No. 1: Before configuration: <pre> FS #show access-lists ip access-list standard 1 10 deny host 50.1.1.2 (10 matches) 20 permit host 60.1.1.2 (15 matches) (10 packets filtered) </pre>	

	After configuration: FS# end FS# clear access-list counters FS# show access-lists ip access-list standard 1 10 deny host 50.1.1.2 (10 matches) 20 permit host 60.1.1.2 (15 matches)	
Related Commands	Command	Description
	expert access-list	Defines an expert ACL.
	deny	Defines a deny ACL entry.
	permit	Defines a permits ACL entry.
Platform Description	N/A	

1.7 deny

	One or multiple deny conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.
	Standard IP ACL
	[sn] deny {source source-wildcard host source any interface idx } [time-range tm-range-name] [log]
	Extended IP ACL
	[sn] deny protocol source source-wildcard destination destination-wildcard [[precedence precedence] [tos tos] [dscp dscp] [ecn ecn]] [fragment] [range lower upper] [time-range time-range-name] [log]
	Extended IP ACLs of some important protocols:
	Internet Control Message Prot (ICMP)
	[sn] deny icmp {source source-wildcard host source any } {destination destination-wildcard host destination any } [icmp-type] [[icmp-type icmp-code]] [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]
	Transmission Control Protocol (TCP)
	[sn] deny tcp { source source-wildcard host Source any } { destination destination-wildcard host destination any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]
	User Datagram Protocol (UDP)
	[sn] deny udp { source source-wildcard host source any } { destination destination-wildcard host destination any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name]
	Extended MAC ACL
	[sn] deny { any host source-mac-address } { any host destination-mac-address } [ethernet-type] [cos [out] [inner in]]
	Extended expert ACL

	<pre>[sn] deny [protocol [ethernet-type] [cos [out] [inner in]]] [[VID [out] [inner in]]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name]</pre>
	When you select the ethernet-type field or cos field:
	<pre>[sn] deny { [ethernet-type] [cos [out] [inner in]] } [[VID [out] [inner in]]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [time-range time-range-name]</pre>
	When you select the protocol field:
	<pre>[sn] deny protocol [[VID [out] [inner in]]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name]</pre>
	Extended expert ACLs of some important protocols
	Internet Control Message Protocol (ICMP)
	<pre>[sn] deny icmp [[VID [out] [inner in]]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [icmp-type] [[icmp-type [icmp-code]] [icmp-message]] [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [time-range time-range-name]</pre>
	Transmission Control Protocol (TCP)
	<pre>[sn] deny tcp [[VID [out] [inner in]]] { source source-wildcard host Source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]</pre>
	User Datagram Protocol (UDP)
	<pre>[sn] deny udp [[VID [out] [inner in]]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name]</pre>
	Address Resolution Protocol (ARP)
	<pre>[sn] deny arp { vid vlan-id } [host source-mac-address any] [host destination-mac-address any] { sender-ip sender-ip-wildcard host sender-ip any } { sender-mac sender-mac-wildcard host sender-mac any } { target-ip target-ip-wildcard host target-ip any }</pre>
	5. Extended IPv6 ACL
	<pre>[sn] deny protocol { source-ipv6-prefix / prefix-length any host source-ipv6-address } { destination-ipv6-prefix / prefix-length any host destination-ipv6-address } [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name]</pre>
	Extended ipv6 ACLs of some important protocols:
	Internet Control Message Protocol (ICMP)
	<pre>[sn] deny icmp { source-ipv6-prefix / prefix-length any source-ipv6-address host } { destination-ipv6-prefix / prefix-length host destination-ipv6-address any } [icmp-type] [[icmp-type [icmp-code]] [icmp-message]] [dscp dscp] [flow-label flow-label] [fragment] [time-range time-range-name]</pre>
	Transmission Control Protocol (TCP)
	<pre>[sn] deny tcp { source-ipv6-prefix / prefix-length host source-ipv6-address any } { destination-ipv6-prefix</pre>

	<pre>/prefix-length host destination-ipv6-address any }] [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]</pre>	
	User Datagram Protocol (UDP)	
	<pre>[sn] deny udp { source-ipv6-prefix/prefix-length host source-ipv6-address any } { destination-ipv6-prefix /prefix-length host destination-ipv6-address any } [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name]</pre>	
Parameter Description	Parameter	Description
	sn	ACL entry sequence number
	deny	If not matched, access is denied.
	source	Specify the source IP address (host address or network address).
	source-wildcard	It can be discontinuous, for example, 0.255.0.32.
	protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
	destination	Specify the destination IP address (host address or network address).
	destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
	fragment	Packet fragment filtering
	precedence	Specify the packet priority.
	precedence	Packet precedence value (0 to 7)
	range	Layer4 port number range of the packet.
	lower	Lower limit of the layer4 port number.
	upper	Upper limit of the layer4 port number.
	time-range	Time range of packet filtering
	time-range-name	Time range name of packet filtering
	tos	Specify type of service.
	tos	ToS value (0 to 15)
	icmp-type	ICMP message type (0 to 255)
	icmp-code	ICMP message type code (0 to 255)
	icmp-message	ICMP message type name
	host source-mac-address	Source physical address
	host destination-mac-address	Destination physical address
	VID vid	Match the specified VID.
	ethernet-type	Ethernet type
	match-all	Match all the bits of the TCP flag.
	tcp-flag	Match the TCP flag.
	established	Match the RST or ACK bits, not other bits of the TCP flag.
	source-ipv6-prefix	Source IPv6 network address or network type
	destination-ipv6-prefix	Destination IPv6 network address or network type
	prefix-length	Prefix mask length

	<i>source-ipv6-address</i>	Source IPv6 address
	<i>destination-ipv6-address</i>	Destination IPv6 address
	<i>dscp</i>	Differential Service Code Point
	<i>dscp</i>	Code value, within the range of 0 to 63
	<i>flow-label</i>	Flow label
	<i>flow-label</i>	Flow label value, within the range of 0 to 1048575.
	<i>protocol</i>	For the IPv6, the field can be ipv6 icmp tcp udp and number in the range 0 to 255
	<i>time-range</i>	Time range of the packet filtering
	<i>time-range-name</i>	Time range name of the packet filtering
Defaults	No entry	
Command mode	ACL configuration mode.	
Usage Guide	Use this command to configure the filtering entry of ACLs in ACL configuration mode.	
Configuration Examples	The following example shows how to create and display an extended expert ACL. This expert ACL denies all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272. <pre> FS(config)#expert access-list extended 2702 FS(config-exp-nacl)#deny tcp host 192.168.4.12 host 0013.0049.8272 any any FS(config-exp-nacl)#permit any any any any FS(config-exp-nacl)#show access-lists expert access-list extended 2702 10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any 20 permit any any any any FS(config-exp-nacl)# </pre> This example shows how to use the extended IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to Interface gigabitethernet 1/1. The configuration procedure is as below: <pre> FS(config)# ip access-list extended ip-ext-acl FS(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any FS(config-ext-nacl)# show access-lists ip access-list extended ip-ext-acl 10 deny tcp host 192.168.4.12 eq 100 any FS(config-ext-nacl)#exit FS(config)#interface gigabitethernet 1/1 FS(config-if)#ip access-group ip-ext-acl in FS(config-if)# </pre> This example shows how to use the extended MAC ACL. The purpose is to deny the host with the MAC address 0013.0049.8272 to send Ethernet frames of the type 100 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:	

```

FS(config)#mac access-list extended mac1
FS(config-mac-nacl)#deny host 0013.0049.8272 any aarp
FS(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
FS(config-mac-nacl)#exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# mac access-group mac1 in

```

This example shows how to use the standard IP ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```

FS(config)#ip access-list standard 34
FS(config-ext-nacl)# deny host 192.168.4.12
FS(config-ext-nacl)#show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
FS(config-ext-nacl)#exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# ip access-group 34 in

```

This example shows how to use the extended IPV6 ACL. The purpose is to deny the host with the IP address 192.168.4.12 and apply the rule to Interface gigabitethernet 1/1. The configuration procedure is as below:

```

FS(config)#ipv6 access-list extended v6-acl
FS(config-ipv6-nacl)#11 deny ipv6 host 192.168.4.12 any
FS(config-ipv6-nacl)#show access-lists
ipv6 access-list extended v6-acl
11 deny ipv6 host 192.168.4.12 any
FS(config-ipv6-nacl)# exit
FS(config)# interface gigabitethernet 1/1
FS(config-if)# ipv6 traffic-filter v6-acl in

```

Related Commands		
	Command	Description
	show access-lists	Displays all ACLs.
	ipv6 traffic-filter	Applies the extended IPv6 ACL on the interface.
	ip access-group	Applies the IP ACL on the interface.
	mac access-group	Applies the extended MAC ACL on the interface.
	ip access-list	Defines an IP ACL.
	mac access-list	Defines an extended MAC ACL.
	expert access-list	Defines an extended expert ACL.
	ipv6 access-list	Defines an extended IPv6 ACL.
	permit	Permits the access.
Platform Description	N/A	

1.8 expert access-group

	Use this command to apply the specified expert access list on the specified interface or globally. Use the no form of the command to remove the application.	
	expert access-group { <i>id</i> <i>name</i> } { in out }	
	no expert access-group { <i>id</i> <i>name</i> } { in out }	
Parameter Description	Parameter	Description
	<i>id</i>	Expert access list number: 2700 to 2899
	<i>name</i>	Name of the expert access list
	in	Specifies filtering on inbound packets.
	out	Specifies filtering on outbound packets.
Defaults	No expert access list is applied on the interface or globally.	
Command mode	Global/Interface configuration mode.	
Usage Guide	This command is used to apply the specified access list globally or on the interface to control the input and output data streams. Use the show access-group command to view the setting. Use the expert access-group { <i>id</i> <i>name</i> } { in out } counter-only command on the interface to only collect packet statistics and not filter packets.	
Configuration Examples	The following example shows how to apply the access-list accept_00d0f8xxxxxx only to Gigabit interface 0/1: <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# expert access-group accept_00d0f8xxxxxx_only in</pre> The following example applies the ACL numbered 2700 on interface fastEthernet0/1 to collect statistics on incoming packets: <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)#expert access-group 2700 in counter-only</pre>	
Related Commands	Command	Description
	show access-group	Displays the ACL configuration.
Platform Description	N/A	

1.9 expert access-list advanced

	Use this command to create an advanced expert access list and place the device in expert advanced access list configuration mode. Use the no form of this command to remove the advanced expert access list.

	expert access-list advanced <i>name</i>	
	no expert access-list advanced <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the advanced expert access list
Defaults	N/A	
Command mode	Global configuration mode	
Usage Guide	Use this command to create an advanced expert access list (namely, ACL80) to match your custom fields.	
Configuration Examples	The following example creates an advanced expert access list named adv-acl. <pre>FS(config)# expert access-list advanced adv-acl FS(config-exp-dacl)# show access-lists expert access-list advanced adv-acl</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
	show access-lists <i>name</i>	Displays the access list of a specified name.
Platform Description	N/A	

1.10 expert access-list extended

	Use this command to create an extended expert access list. Use the no form of the command to remove the ACL.	
	expert access-list extended <i>{id name}</i>	
	no expert access-list extended <i>{id name}</i>	
Parameter Description	Parameter	Description
	<i>id</i>	Extended expert access list number: 2700 to 2899
	<i>name</i>	Name of the extended expert access list
Defaults	N/A	
Command mode	Global configuration mode.	

Usage Guide	Use the show access-lists command to display the ACL configurations.	
Configuration Examples	Create an extended expert ACL named exp-acl: <pre>FS(config)# expert access-list extended exp-acl FS(config-exp-nacl)# show access-lists expert access-list extended exp-acl FS(config-exp-nacl)#</pre> Create an extended expert ACL numbered 2704: <pre>FS(config)# expert access-list extended 2704 FS(config-exp-nacl)# show access-lists access-list extended 2704 FS(config-exp-nacl)#</pre>	
Related Commands	Command	Description
	show access-lists	Displays the extended expert ACLs
Platform Description	N/A	

1.11 expert access-list counter

	Use this command to enable the counter of packets matching the specified expert access list. Use the no form of this command to disable this function.	
	expert access-list counter { <i>id</i> <i>name</i> }	
	no expert access-list counter { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	Expert access list number: 2700 to 2899.
	<i>name</i>	Name of the access list.
Defaults	The counter of the packets matching the expert access list is disabled.	
Command mode	Global configuration mode	
Usage Guide	Use this command to enable the counter of packets matching the specified expert access list, so that you can analyze the counters to learn whether the network is attacked by the illegal packets.	
Configuration Examples	The following example enables the counter of packets matching the extended expert access list named exp-acl: <pre>FS(config)# expert access-list counter exp-acl FS(config)# show access-lists expert access-list extended exp-acl 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any (16 matches) 20 deny tcp any any eq login any any (78 matches)</pre>	

	The following example disables the counter of packets matching the extended expert access list named exp-acl. <pre>FS(config)#no expert access-list counter exp-acl FS(config)# show access-lists expert access-list extended 2700 10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any 20 deny tcp any any eq login any any</pre>	
Related Commands	Command	Description
	show access-lists	Displays the extended expert ACL.
Platform Description	N/A	

1.12 expert access-list new-fragment-mode

	Use this command to switch the matching mode of fragmentation packets. Use the no form of this command to restore the default matching mode of fragmentation packets.	
	expert access-list new-fragment-mode { id name }	
	no expert access-list new-fragment-mode { id name }	
Parameter Description	Parameter	Description
	<i>id</i>	Expert access list number: 2700 to 2899.
	<i>name</i>	Name of the expert access list.
Defaults	Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.	
Command mode	Global configuration mode	
Usage Guide	Use this command to switch and control the matching mode of access rules to fragmentation packets.	
Configuration Examples	The following example switches the matching mode of fragmentation packets for the ACL 2700 from the default mode to a new matching mode: <pre>FS(config)#expert access-list new-fragment-mode 2700</pre>	
Related Commands	Command	Description
	-	-
Platform Description	N/A	

1.13 expert access-list resequence

	Use this command to resequence an expert access list. Use the no form of this command to restore the default order of access entries.	
	expert access-list resequence { <i>id</i> <i>name</i> } <i>start-sn</i> <i>inc-sn</i>	
	no expert access-list resequence { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	Expert access list number: 2700 to 2899.
	<i>name</i>	Name of the expert access list
	<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
	<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647
Defaults	<i>start-sn</i> : 10 <i>inc-sn</i> : 10	
Command mode	Global configuration mode	
Usage Guide	Use this command to change the order of the access entries.	
Configuration Examples	The following example resequences entries of expert access list "exp-acl": Before the configuration: <pre>FS# show access-lists expert access-list extended exp-acl 10 permit ip any any any any 20 deny ip any any any any</pre> After the configuration: <pre>FS# config FS(config)# expert access-list resequence exp-acl 21 43 FS(config)# exit FS# show access-lists expert access-list extended exp-acl 21 permit ip any any any any 64 deny ip any any any any</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists..
Platform Description	N/A	

1.14 global access-group

	Use this command to apply the global access list on the interface. Use the no form of this command to remove the global access list from the interface.	
	global access-group	
	no global access-group	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the global access list is applied on the interface.	
Command mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example applies the global access list on interface fastEthernet0/0. <pre>FS(config)# interface fastEthernet 0/0 FS(config-if-GigabitEthernet 0/0)#global access-group</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.15 ip access-group

	Use this command to apply a specific access list globally or to an interface. Use the no form of this command to remove the access list from the interface.	
	ip access-group {id name} {in out}	
	no ip access-group {id name} {in out}	
Parameter Description	Parameter	Description
	<i>id</i>	IP access list or extended IP access list number: 1 to 199, 1300 to 2699
	<i>name</i>	Name of the IP ACL
	<i>in</i>	Filters the incoming packets of the interface.
	<i>out</i>	Filters the outgoing packets of the interface.

Defaults	No access list is applied globally or on the interface by default.	
Command mode	Global, interface	
Usage Guide	Use this command to control access to a specified interface, VXLAN or globally.	
Configuration Examples	The following example applies the ACL 120 on interface fastEthernet0/0 to filter the incoming packets: <pre>FS(config)# interface fastEthernet 0/0 FS(config-if)# ip access-group 120 in</pre>	
Related Commands	Command	Description
	access-list	Defines an ACL.
	show access-lists	Displays all ACLs.
Platform Description	N/A	

1.16 ip access-list

	Use this command to create a standard IP access list or extended IP access list. Use the no form of the command to remove the access list.	
	ip access-list { extended standard } { <i>id</i> <i>name</i> }	
	no ip access-list { extended standard } { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number: Standard: 1 to 99, 1300 to 1999; Extended: 100 to 199, 2000 to 2699.
	<i>name</i>	Name of the access list
Defaults	N/A	
Command mode	Global configuration mode	
Usage Guide	Configure a standard access list if you need to filter on source address only. If you want to filter on anything other than source address, you need to create an extended access list. Refer to deny or permit in the two modes. Use the show access-lists command to display the ACL configurations.	
Configuration	The following example creates a standard access list named std-acl.	

Examples	<pre>FS(config)# ip access-list standard std-acl FS(config-std-nacl)# show access-lists ip access-list standard std-acl FS(config-std-nacl)#</pre>	
	The following example creates an extended ACL numbered 123: <pre>FS(config)# ip access-list extended 123 FS(config-ext-nacl)# show access-lists ip access-list extended 123</pre>	
Related Commands	Command	Description
	show access-lists	Displays all ACLs.
Platform Description	N/A	

1.17 ip access-list log-update interval

	Use this command to configure the interval at which the IPv4 access list log is updated. Use the no form of this command to restore the default interval.	
	ip access-list log-update interval <i>time</i>	
	no ip access-list log-update interval	
Parameter Description	Parameter	Description
	<i>time</i>	For the access rule with the log option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specified flow is output every 5 minutes. 0 indicates that no ACL logging is output.
Defaults	The default interval at which the IPv4 access list log is updated is 5 minutes.	
Command mode	Global configuration mode	
Usage Guide	Use this command to configure the interval at which the IPv4 access list log is updated.	
Configuration Examples	The following example configures the interval for the IPv4 access list log update to 10 minutes: <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ip access-list log-update interval 10</pre>	

Related Commands	Command	Description
	ip access-list	Defines an IPv4 access list.
	deny	Defines the deny access entries.
	permit	Defines the permit access entries.
	show running	Displays running configurations of the device.
Platform Description	N/A	

1.18 ip access-list counter

	Use this command to enable the counter of packets matching the standard or extended IP access list. Use the no form of this command to disable the counter.	
	ip access-list counter { <i>id</i> <i>name</i> }	
	no ip access-list counter { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
	<i>name</i>	Name of the IP access list.
Defaults	The counter of packets matching the standard or extended IP access list is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the counter of packets matching the standard access list: <pre>FS(config)# ip access-list counter std-acl FS(config-std-nacl)# show access-lists ip access-list standard std-acl 10 permit 195.168.6.0 0.0.0.255 (999 matches) 20 deny host 5.5.5.5 time-range tm (2000 matches)</pre> The following example disables the counter of packets matching the standard access list: <pre>FS(config)#no ip access-list counter std-acl FS(config-std-nacl)# show access-lists ip access-list standard std-acl 10 permit 195.168.6.0 0.0.0.255 20 deny host 5.5.5.5 time-range tm</pre>	

Related Commands	Command	Description
	show access-lists	Displays all access lists.
Platform Description	N/A	

1.19 ip access-list new-fragment-mode

	Use this command to switch the matching mode of fragmentation packets of standard or extended IP access list. Use the no form of this command to restore the default matching mode of fragmentation packets.	
	ip access-list new-fragment-mode { <i>id</i> <i>name</i> }	
	no ip access-list new-fragment-mode { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
	<i>name</i>	Name of the standard or extended IP access list
Defaults	Use the default matching mode of fragmentation packets. By default, if the access rule is tagged with fragment, it will match all packets except for the first fragmentation packet. If the access rule is not tagged with fragment, all packets including the first and all subsequent fragmentation packets will be matched.	
Command mode	Global configuration mode	
Usage Guide	This command is used to switch and control the fragmentation packet matching mode of access rules.	
Configuration Examples	The following example switches the fragmentation packet matching mode of the ACL 100 from the default mode to a new mode: <pre>FS(config)#ip access-list new-fragment-mode 100</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.20 ip access-list resequence

	Use this command to resequence a standard or extended IP access list. Use the no form of this command to restore the default order of access entries.	
	ip access-list resequence { <i>id</i> <i>name</i> } <i>start-sn</i> <i>inc-sn</i>	
	no ip access-list resequence { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	IP access list number: Standard IP access list: 1 to 99, 1300 to 1999; Extended IP access list: 100 to 199, 2000 to 2699.
	<i>name</i>	Name of the standard or extended IP access list
	<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
	<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647
Defaults	<i>start-sn</i> : 10 <i>inc-sn</i> : 10	
Command mode	Global configuration mode	
Usage Guide	Use this command to change the order of the access entries.	
Configuration Examples	The following example resequences entries of ACL1: Before the configuration: <pre>FS# show access-lists ip access-list standard 1 10 permit host 192.168.4.12 20 deny any any</pre> After the configuration: <pre>FS# config FS(config)# ip access-list resequence 1 21 43 FS(config)# exit FS# show access-lists ip access-list standard 1 21 permit host 192.168.4.12 64 deny any any</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists..

Platform	N/A
Description	

1.21 ipv6 access-list

	Use this command to create an IPv6 access list and to place the device in IPv6 access list configuration mode. Use the no form of this command to remove the access list.	
	ipv6 access-list <i>name</i>	
	no ipv6 access-list <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the IPv6 access list.
Defaults	N/A	
Command mode	Global configuration mode	
Usage Guide	To filter the IPv6 packets through the access list, you need to define an IPv6 access list by using the ipv6 access-list command.	
Configuration Examples	The following example creates an IPv6 access list named v6-acl: <pre>FS(config)# ipv6 access-list v6-acl FS(config-ipv6-nacl)# show access-lists ipv6 access-list extended v6-acl FS(config-ipv6-nacl)#</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
Platform	N/A	
Description		

1.22 ipv6 access-list counter

	Use this command to enable the counter of packets matching the IPv6 access list. Use the no form of this command to disable the counter.	
	ipv6 access-list counter <i>name</i>	
	no ipv6 access-list counter <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the IPv6 access list.

Defaults	-				
Command mode	Global configuration mode				
Usage Guide	Use this command to enable the counter of packets matching the IPv6 access list to monitor the IPv6 packets matching and filtering.				
Configuration Examples	The following example enables the counter of packets matching the IPv6 access list named v6-acl: <pre>FS(config)# ipv6 access-list v6-acl FS(config-ipv6-nacl)# show access-lists ipv6 access-list acl-v6 10 permit icmp any any (7 matches) 20 deny tcp any any (7 matches)</pre> The following example disables the counter of packets matching the IPv6 access list named v6-acl: <pre>FS(config)#no ipv6 access-list v6-acl counter FS(config-ipv6-nacl)# show access-lists ipv6 access-list acl-v6 10 permit icmp any any 20 deny tcp any any</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show access-lists</td><td>Displays all access lists.</td></tr> </table>	Command	Description	show access-lists	Displays all access lists.
Command	Description				
show access-lists	Displays all access lists.				
Platform Description	N/A				

1.23 ipv6 access-list log-update interval

	Use this command to configure the interval at which the IPv6 access list log is updated. Use the no form of this command to restore the default interval.	
	ipv6 access-list log-update interval time	
	no ipv6 access-list log-update interval	
Parameter Description	Parameter	Description
	<i>time</i>	For the access rule with the logging option, a packet hit is output at the interval of ACL logging output. The interval ranges from 0 to 1440 minutes, and the default value is 5 minutes, indicating that the ACL matching log of a specific flow is output every 5 minutes. 0 indicates that no ACL logging is output.

Defaults	By default, the value is 5 minutes.										
Command mode	Global configuration mode										
Usage Guide	Use this command to configure the interval at which the IPv6 access list log is updated.										
Configuration Examples	The following example configures the interval for the IPv6 access list log update to 10 minutes: <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# ipv6 access-list log-update interval 9</pre>										
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ipv6 access-list</td><td>Defines an IPv6 access list.</td></tr> <tr> <td>deny</td><td>Defines the deny access entries.</td></tr> <tr> <td>permit</td><td>Defines the permit access entries.</td></tr> <tr> <td>show running</td><td>Displays the running configurations of the device.</td></tr> </table>	Command	Description	ipv6 access-list	Defines an IPv6 access list.	deny	Defines the deny access entries.	permit	Defines the permit access entries.	show running	Displays the running configurations of the device.
Command	Description										
ipv6 access-list	Defines an IPv6 access list.										
deny	Defines the deny access entries.										
permit	Defines the permit access entries.										
show running	Displays the running configurations of the device.										
Platform Description	N/A										

1.24 ipv6 access-list resequence

	Use this command to resequence an IPv6 access list. Use the no form of this command to restore the default order of access entries.	
	ipv6 access-list resequence <i>name start-sn inc-sn</i>	
	no ipv6 access-list resequence <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the IPv6 access list
	<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
	<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647
Defaults	<i>start-sn</i> : 10 <i>inc-sn</i> : 10	
Command mode	Global configuration mode	
Usage Guide	Use this command to change the order of the access entries.	

Configuration Examples	The following example resequences entries of IPv6 access list "v6-acl":	
	Before the configuration: <pre>FS# show access-lists ipv6 access-list v6-acl 10 permit ipv6 any any 20 deny ipv6 any any</pre> After the configuration: <pre>FS# config FS(config)# ipv6 access-list resequence v6-acl 21 43 FS(config)# exit FS# show access-lists ipv6 access-list v6-acl 21 permit ipv6 any any 64 deny ipv6 any any</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists..
Platform Description	N/A	

1.25 ipv6 traffic-filter

	Use this command to apply an IPV6 access list on the specified interface/VXLAN. Use the no form of the command to remove the IPv6 access list from the interface.	
	ipv6 traffic-filter <i>name</i> { in out }	
	no ipv6 traffic-filter <i>name</i> { in out }	
Parameter Description	Parameter	Description
	<i>name</i>	Name of IPv6 access list
	in	Specifies filtering on inbound packets
	out	Specifies filtering on outbound packets
Defaults	N/A	
Command mode	Interface configuration mode.	
Usage Guide	Use this command to apply the IPv6 access list to a specified interface to filter the inbound or outbound packets.	
Configuration	The following example applies the IPv6 access list named v6-acl to interface GigabitEthernet 0/1:	

Examples	<pre>FS(config)# interface GigaEthernet 0/1 FS(config-if)# ipv6 traffic-filter v6-acl in</pre>	
Related Commands	Command	Description
	show access-group	Displays ACL configurations on the interface.
Platform Description	N/A	

1.26 list-remark

	Use this command to write a helpful comment (remark) for an access list. Use the no form of this command to remove the remark.	
	list-remark <i>text</i>	
	no list-remark	
Parameter Description	Parameter	Description
	<i>text</i>	Comment that describes the access list.
Defaults	The access lists have no remarks by default.	
Command mode	ACL configuration mode	
Usage Guide	You can use this command to write a helpful comment for a specified access list.	
Configuration Examples	The following example writes a comment of "this acl is to filter the host 192.168.4.12" for ACL102. <pre>FS(config)# ip access-list extended 102 FS(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12 FS(config-ext-nacl)# show access-lists ip access-list extended 102 deny ip host 192.168.4.12 any 1000 hits this acl is to filter the host 192.168.4.12 FS(config-ext-nacl)#</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
	ip access-list	Defines an IPv4 access list.
	access-list list remark	Adds a helpful comment for an access list in global configuration mode.

Platform	N/A
Description	

1.27 mac access-group

	Use this command to apply the specified MAC access list globally or on the specified interface.. Use the no form of the command to remove the access list from the interface.	
	mac access-group { <i>id</i> <i>name</i> } { in out }	
	no mac access-group { <i>id</i> <i>name</i> } { in out }	
Parameter Description	Parameter	Description
	<i>id</i>	MAC access list number. The range is from 700 to 799.
	<i>name</i>	Name of the MAC access list
	in	Specifies filtering on the inbound packets.
	out	Specifies filtering on the outbound packets.
Defaults	No MAC access list is applied by default.	
Command mode	Global/Interface configuration mode.	
Usage Guide	Use this command to apply the access list globally or to the interface to filter the inbound or outbound packets based on the MAC address.	
Configuration Examples	The following example applies the MAC access-list accept_00d0f8xxxxxx_only to interface GigabitEthernet 1/1: <pre>FS(config)# interface GigaEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# mac access-group accept_00d0f8xxxxxx_only in</pre>	
Related Commands	Command	Description
	show access-group	Displays the ACL configuration on the interface.
Platform	N/A	
Description		

1.28 mac access-list extended

	Use this command to create an extended MAC access list. Use the no form of the command to remove the MAC access list.
	mac access-list extended { <i>id</i> <i>name</i> }
	no mac access-list extended { <i>id</i> <i>name</i> }

Parameter Description	Parameter	Description
	<i>id</i>	Extended MAC access list number. The range is from 700 to 799.
	<i>name</i>	Name of the extended MAC access list
Defaults	N/A	
Command mode	Global configuration mode.	
Usage Guide	To filter the packets based on the MAC address, you need to define a MAC access list by using the mac access-list extended command.	
Configuration Examples	The following command creates an extended MAC access list named mac-acl: <pre>FS(config)# mac access-list extended mac-acl</pre> FS(config-mac-nacl)# show access-lists mac access-list extended mac-acl The following command creates an extended MAC access list numbered 704: <pre>FS(config)# mac access-list extended 704</pre> FS(config-mac-nacl)# show access-lists mac access-list extended 704	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
Platform Description	N/A	

1.29 mac access-list counter

	Use this command to enable the counter of packet matching the extended MAC access list. Use the no form of this command to disable the counter.	
	mac access-list counter { <i>id</i> <i>name</i> }	
	no mac access-list counter { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	Extended MAC access list number. The range is from 700 to 799.
	<i>name</i>	Name of the extended MAC access list
Defaults	The counter is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	Use this command to enable the counter of packets matching the MAC access list to monitor the packets	

	matching and filtering.	
Configuration Examples	The following example enables the counter of packet matching the extended MAC access list named mac-acl: <pre>FS(config)# mac access-list counter mac-acl FS(config)# show access-lists mac access-list extended mac-acl 10 permit host 0023.56ac.8965 any (170 matches) 20 deny any any etype-any cos 6 (239 matches)</pre> The following example disables the counter of packet matching the extended MAC access list named mac-acl: <pre>FS(config)# no mac access-list counter mac-acl FS(config)# show access-lists mac access-list extended mac-acl 10 permit host 0023.56ac.8965 any 20 deny any any etype-any cos 6</pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
Platform Description	N/A	

1.30 mac access-list resequence

	Use this command to resequence an extended MAC access list. Use the no form of this command to restore the default order of access entries.	
	mac access-list resequence { <i>id</i> <i>name</i> } <i>start-sn</i> <i>inc-sn</i>	
	no mac access-list resequence { <i>id</i> <i>name</i> }	
Parameter Description	Parameter	Description
	<i>id</i>	Extended MAC access list number: 700 to 799.
	<i>name</i>	Name of the extended MAC access list
	<i>start-sn</i>	Start sequence number. Range: 1 to 2147483647
	<i>inc-sn</i>	Increment of the sequence number. Range: 1 to 2147483647
Defaults	<i>start-sn</i> : 10 <i>inc-sn</i> : 10	
Command mode	Global configuration mode	
Usage Guide	Use this command to change the order of the access entries.	

Configuration Examples	The following example resequences entries of extended MAC access list "mac-acl": Before the configuration: <pre>FS# show access-lists mac access-list extended mac-acl 10 permit any any etype-any 20 deny any any etype-any</pre> After the configuration: <pre>FS# config FS(config)# mac access-list resequence exp-acl 21 43 FS(config)# exit FS# show access-lists mac access-list extended mac-acl 21 permit any any etype-any 64 deny any any etype-any</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>show access-lists</td><td>Displays all access lists..</td></tr> </tbody> </table>	Command	Description	show access-lists	Displays all access lists..
Command	Description				
show access-lists	Displays all access lists..				
Platform Description	N/A				

1.31 permit

	One or multiple permit conditions are used to determine whether to forward or discard the packet. In ACL configuration mode, you can modify the existent ACL or configure according to the protocol details.
	Standard IP ACL
	<code>[sn] permit { source source-wildcard host source any interface idx } [time-range tm-range-name] [log]</code>
	Extended IP ACL
	<code>[sn] permit protocol source source-wildcard destination destination-wildcard [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name] [log]</code>
	Extended IP ACLs of some important protocols:
	Internet Control Message Protocol (ICMP)
	<code>[sn] permit icmp { source source-wildcard host source any } { destination destination-wildcard host destination any } [icmp-type] [[icmp-type [icmp-code]] [icmp-message]] [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [time-range time-range-name]</code>
	Transmission Control Protocol (TCP)
	<code>[sn] permit tcp { source source-wildcard host Source any } { destination destination-wildcard host destination any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]</code>
	User Datagram Protocol (UDP)
	<code>[sn] permit udp { source source -wildcard host source any } { destination destination-wildcard</code>

	host destination any } [precedence precedence] [tos tos] [dscp dscp] [fragment] [range lower upper] [time-range time-range-name]
	Extended MAC ACL
	[sn] permit { any host source-mac-address source-mac-address mask } { any host destination-mac-address destination-mac-address mask } [ethernet-type] [cos [out] [inner in]]
	Extended expert ACL
	[sn] permit [protocol] [ethernet-type] [cos [out] [inner in]] [VID [out] [inner in]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [precedence precedence] [tos tos] [dscp dscp] [fragment] [range lower upper] [time-range time-range-name]
	When you select the Ethernet-type field or cos field:
	[sn] permit { ethernet-type cos [out] [inner in] } [VID [out] [inner in]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [time-range time-range-name]
	When you select the protocol field:
	[sn] permit protocol [VID [out] [inner in]] { source source-wildcard host Source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [precedence precedence] [tos tos] [dscp dscp] [fragment] [range lower upper] [time-range time-range-name]
	Extended expert ACLs of some important protocols:
	Internet Control Message Protocol (ICMP)
	[sn] permit icmp [VID [out] [inner in]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [icmp-type] [[icmp-type icmp-code]] [icmp-message] [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [time-range time-range-name]
	Transmission Control Protocol (TCP)
	[sn] permit tcp [VID [out] [inner in]] { source source-wildcard host Source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]
	User Datagram Protocol (UDP)
	[sn] permit udp [VID [out] [inner in]] { source source-wildcard host source any } { host source-mac-address any } { destination destination-wildcard host destination any } { host destination-mac-address any } [[precedence precedence] [tos tos] [dscp dscp]] [fragment] [range lower upper] [time-range time-range-name]
	Address Resolution Protocol (ARP)
	[sn] permit arp { vid vlan-id } { host source-mac-address any } { host destination-mac-address any } { sender-ip sender-ip-wildcard host sender-ip any } { sender-mac sender-mac-wildcard host sender-mac any } { target-ip target-ip-wildcard host target-ip any }
	Extended IPv6 ACL
	[sn] permit protocol { source-ipv6-prefix / prefix-length any host source-ipv6-address } { destination-ipv6-prefix / prefix-length any host destination-ipv6-address } [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name]
	Extended IPv6 ACLs of some important protocols:

	Internet Control Message Protocol (ICMP)	
	[sn] permit icmp {source-ipv6-prefix / prefix-length any source-ipv6-address host } {destination-ipv6-prefix / prefix-length host destination-ipv6-address any } [icmp-type] [[icmp-type [icmp-code]] [icmp-message]] [dscp dscp] [flow-label flow-label][fragment] [time-range time-range-name]	
	Transmission Control Protocol (TCP)	
	[sn] permit tcp { source-ipv6-prefix / prefix-length host source-ipv6-address any } { destination-ipv6-prefix / prefix-length host destination-ipv6-address any } [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag established]	
	User Datagram Protocol (UDP)	
	[sn] permit udp { source-ipv6-prefix / prefix-length host source-ipv6-address any } { destination-ipv6-prefix / prefix-length host destination-ipv6-address any } [dscp dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name]	
Parameter Description	Parameter	Description
	sn	ACL entry sequence number
	permit	If matched, access is permitted.
	source	Specify the source IP address (host address or network address).
	source-wildcard	It can be discontinuous, for example, 0.255.0.32.
	protocol	IP protocol number. It can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, and IP. It can also be a number representing the IP protocol between 0 and 255. The important protocols such as ICMP, TCP, and UDP are described separately.
	destination	Specify the destination IP address (host address or network address).
	destination-wildcard	Wildcard of the destination IP address. It can be discontinuous, for example, 0.255.0.32.
	fragment	Packet fragment filtering
	precedence	Specify the packet priority.
	precedence	Packet precedence value (0 to 7)
	range	Layer4 port number range of the packet.
	lower	Lower limit of the layer4 port number.
	upper	Upper limit of the layer4 port number.
	time-range	Time range of packet filtering
	time-range-name	Time range name of packet filtering
	tos	Specify type of service.
	tos	ToS value (0 to 15)
	icmp-type	ICMP message type (0 to 255)
	icmp-code	ICMP message type code (0 to 255)
	icmp-message	ICMP message type name
	host source-mac-address	Source physical address
	host destination-mac-address	Destination physical address
	VID vid	Match the specified VID.
	ethernet-type	Ethernet type

	match-all	Match all the bits of the TCP flag.
	tcp-flag	Match the TCP flag.
	established	Match the RST or ACK bits, not other bits of the TCP flag.
	source-ipv6-prefix	Source IPv6 network address or network type
	destination-ipv6-prefix	Destination IPv6 network address or network type
	prefix-length	Prefix mask length
	source-ipv6-address	Source IPv6 address
	destination-ipv6-address	Destination IPv6 address
	dscp	Differential Service Code Point
	dscp	Code value, within the range of 0 to 63
	flow-label	Flow label
	flow-label	Flow label value, within the range of 0 to 1048575.
	protocol	For the IPv6, the field can be ipv6 icmp tcp udp and number in the range 0 to 255
	time-range	Time range of the packet filtering
	time-range-name	Time range name of the packet filtering
Defaults	N/A	
Command mode	ACL configuration mode.	
Usage Guide	Use this command to configure the permit conditions for the ACL in ACL configuration mode.	
Configuration Examples	The following example shows how to create and display an Expert Extended ACL. This expert ACL permits all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 001300498272. <pre> FS(config)#expert access-list extended exp-acl FS(config-exp-nacl)#permit tcp host 192.168.4.12 host 0013.0049.8272 any any FS(config-exp-nacl)#deny any any any any FS(config-exp-nacl)#show access-lists expert access-list extended exp-acl 10 permit tcp host 192.168.4.12 host 0013.0049.8272 any any 20 deny any any any any FS(config-exp-nacl)# </pre> This example shows how to use the extended IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 to provide services through the TCP port 100 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below: <pre> FS(config)# ip access-list extended 102 FS(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any FS(config-ext-nacl)# show access-lists ip access-list extended 102 10 permit tcp host 192.168.4.12 eq 100 any FS(config-ext-nacl)#exit FS(config)#interface gigabitethernet 1/1 </pre>	

```
FS(config-if)#ip access-group 102 in
```

```
FS(config-if)#
```

This example shows how to use the extended MAC ACL. The purpose is to permit the host with the MAC address 0013.0049.8272 to send Ethernet frames through the type 100 and apply the ACL to interface gigabitethernet 1/1.

The configuration procedure is as below:

```
FS(config)#mac access-list extended 702
```

```
FS(config-mac-nacl)#permit host 0013.0049.8272 any aarp
```

```
FS(config-mac-nacl)#show access-lists
```

```
mac access-list extended 702
```

```
10 permit host 0013.0049.8272 any aarp 702
```

```
FS(config-mac-nacl)#exit
```

```
FS(config)#interface gigabitethernet 1/1
```

```
FS(config-if)#mac access-group 702 in
```

This example shows how to use the standard IP ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#ip access-list standard std-acl
```

```
FS(config-std-nacl)#permit host 192.168.4.12
```

```
FS(config-std-nacl)#show access-lists
```

```
ip access-list standard std-acl
```

```
10 permit host 192.168.4.12
```

```
FS(config-std-nacl)#exit
```

```
FS(config)# interface gigabitethernet 1/1
```

```
FS(config-if)# ip access-group std-acl in
```

This example shows how to use the extended IPV6 ACL. The purpose is to permit the host with the IP address 192.168.4.12 and apply the ACL to interface gigabitethernet 1/1. The configuration procedure is as below:

```
FS(config)#ipv6 access-list extended v6-acl
```

```
FS(config-ipv6-nacl)#11 permit ipv6 host ::192.168.4.12 any
```

```
FS(config-ipv6-nacl)# show access-lists
```

```
ipv6 access-list extended v6-acl
```

```
11 permit ipv6 host ::192.168.4.12 any
```

```
FS(config-ipv6-nacl)# exit
```

```
FS(config)#interface gigabitethernet 1/1
```

```
FS(config-if)#ipv6 traffic-filter v6-acl in
```

Related Commands	Command	Description
	show access-lists	Displays all access lists.
	ipv6 traffic-filter	Applies the extended IPv6 access list to the interface.
	ip access-group	Applies the IP access list to the interface.
	mac access-group	Applies the extended MAC access list to the interface.
	ip access-list	Defines an IP access list.
	mac access-list	Defines an extended MAC access list.
	expert access-list	Define an extended expert access list.
	ipv6 access-list	Defines an extended IPv6 access list.

	deny	Defines the deny access entry.
Platform	N/A	
Description		

1.32 redirect destination interface

	Use this command to redirect the traffic matching the access list to the specified interface. Use the no form of this command to remove the redirection.	
	redirect destination interface <i>interface-name</i> acl { <i>id</i> <i>name</i> } in	
	no redirect destination interface <i>interface-name</i> acl { <i>id</i> <i>name</i> } in	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Redirect interface
	<i>id</i>	Access list number
	<i>name</i>	Access list name
Defaults	No redirection is configured.	
Command mode	Interface configuration mode	
Usage Guide	Use this command to configure access redirection, namely, to redirect the traffic matching the access list to the specified interface. You can monitor the operation of a specified access list by using this command.	
Configuration Examples	The following example configures access redirection. <pre>FS(config)# interface gigabitEthernet 0/3 FS(config-if-GigabitEthernet 0/3)# redirect destination interface gigabitEthernet 0/2 acl1 in</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

1.33 remark

	Use this command to write a helpful comment (remark) for an entry in the access list. Use the no form of this command to remove the remark.
	<i>[sn]</i> remark <i>text</i>
	no <i>[sn]</i> remark

Parameter Description	Parameter	Description
	<i>text</i>	Comment that describes the access entry.
	<i>sn</i>	The sequence number of the ACE.
Defaults	The access entries have no remarks.	
Command mode	ACL configuration mode.	
Usage Guide	Use this command to write a helpful comment for an access entry. Up to 100 characters are allowed in the remark. Two access entry remarks in one access list entry are not allowed. Removing an access entry may delete the remark for it as well. If <i>sn</i> is specified, the remark is applied to the specified ACE; otherwise, the remark is applied to the last ACE.	
Configuration Examples	The following example writes remarks for the entry in extended IP access list 102. <pre> FS(config)# ip access-list extended 102 FS(config-ext-nacl)# remark first_remark FS(config-ext-nacl)# 10 permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0 FS(config-ext-nacl)# 10 remark second_remark FS(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0 FS(config-ext-nacl)# end FS# </pre>	
Related Commands	Command	Description
	show access-lists	Displays all access lists.
	ip access-list	Defines an IP access list.
Platform Description	N/A	

11.12 security access-group

	Use this command to configure an interface secure channel. Use the no form of this command to restore to default settings.	
	security access-group { <i>id</i> <i>name</i> }	
	no security access-group	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number.

	<i>name</i>	Name of the access list.
Defaults	N/A	
Command mode	Interface configuration mode	
Usage Guide	If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a secure channel for the users on the specified interface to access the external network without authentication.	
Configuration Examples	The following example configures a secure channel on interface GigaEthernet 1/1: <pre>FS(config)# interface GigaEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# security access-group 1</pre>	
Related Commands	Command	Description
	show secu-acl	Displays the secure channel configuration.
Platform Description	N/A	

1.34 security global access-group

	Use this command to configure the global secure channel.	
	security global access-group { <i>id</i> <i>name</i> }	
	no security global access-group	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number.
	<i>name</i>	Name of the access list.
Defaults	-	
Command mode	Global configuration mode	
Usage Guide	If a device is configured authentications such as 802.1x or Web authentication, the user cannot access the external network before passing the authentication. You can use this command to configure a global secure channel for some users to access the external network without authentication.	
Configuration Examples	The following example configures a global secure channel. <pre>FS(config)#security global access-group 1</pre>	

Related Commands	Command	Description
	show secu-acl	Displays the secure channel configuration..
Platform Description	N/A	

1.35 security uplink enable

	Use this command to configure an exceptional interface of the global secure channel.	
	security uplink enable	
	no security uplink enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The global secure channel takes effect on all interfaces by default.	
Command mode	Interface configuration mode.	
Usage Guide	The global secure channel takes effect on all interfaces by default. To disable the secure channel function on some interfaces, you can use this command to configure the interface as exceptional.	
Configuration Examples	The following example configures interface GigaEthernet 1/1 as an exceptional interface of the secure channel. <pre>FS(config)# interface GigaEthernet 1/1 FS(config-if-GigabitEthernet 1/1)# security uplink enable</pre>	
Related Commands	Command	Description
	show secu-acl	Displays the secure channel configuration.
Platform Description	N/A	

1.36 show access-group

	Use this command to display the access list applied to the interface.
	show access-group [interface interface-name]

Parameter Description	Parameter	Description
	<i>interface</i>	Interface name
Defaults	-	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the access list configuration on the specified interface. If no interface is specified, access list configuration on all interfaces is displayed.	
Configuration Examples	FS# show access-group ip access-list standard ipstd3 Applied On interface GigabitEthernet 0/1. ip access-list standard ipstd4 Applied On interface GigabitEthernet 0/2. ip access-list extended 101 Applied On interface GigabitEthernet 0/3. ip access-list extended 102 Applied On interface GigabitEthernet 0/8.	
Related Commands	Command	Description
	ip access-group	Applies the IP access list to the interface.
	mac access-group	Applies the MAC access list to the interface.
	expert access-group	Applies the expert access list to the interface.
	ipv6 traffic-filter	Applies the IPv6 access list to the interface.
Platform Description	N/A	

1.37 show access-lists

	Use this command to display all access lists or the specified access list.	
	show access-lists [<i>id</i> <i>name</i>] [summary]	
Parameter Description	Parameter	Description
	<i>id</i>	Access list number
	<i>name</i>	Name of the IP access list
	summary	Access list summary

Defaults	N/A	
Command mode	Global configuration mode	
Usage Guide	Use this command to display the specified access list. If no access list number or name is specified, all the access lists are displayed.	
Configuration Examples	<pre> FS# show access-lists n_acl ip access-list standard n_acl FS# show access-lists 102 ip access-list extended 102 FS# show access-lists ip access-list standard n_acl ip access-list extended 101 permit icmp host 192.168.1.1 any log (1080 matches) permit tcp host 1.1.1.1 any established deny ip any any (80021 matches) mac access-list extended mac_acl expert access-list extended exp_acl ipv6 access-list extended v6_acl petmit ipv6 ::192.168.4.12 any (100 matches) deny any any (9 matches) </pre>	
Related Commands	Command	Description
	ip access-list	Defines an IP access list.
	mac access-list	Defines an extended MAC access list.
	expert access-list	Defines an extended expert access list.
	ipv6 access-list	Defines an extended IPv6 access list.
Platform Description	N/A	

1.38 show expert access-group

	Use this command to display the expert access list applied to the interface.	
	show expert access-group [interface interface-name]	
Parameter Description	Parameter	Description
	interface-name	Interface name

Defaults	-	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the expert access list configured on the interface. If no interface is specified, the expert access lists on all interfaces are displayed.	
Configuration Examples	FS# show expert access-group interface gigabitethernet 0/2 expert access-group ee in Applied On interface GigabitEthernet 0/2.	
Related Commands	Command	Description
	expert access-list	Defines an extended expert access list.
Platform Description	N/A	

1.39 show ip access-group

	Use this command to display the standard and extended IP access lists on the interface.	
	show ip access-group [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>Interface Interface-name</i>	Interface name
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the standard and extended IP access lists configured on the interface. If no interface is specified, the standard and extended IP access lists on all interfaces are displayed.	
Configuration Examples	FS# show ip access-group interface gigabitethernet 0/1 ip access-group aaa in Applied On interface GigabitEthernet 0/1.	
Related Commands	Command	Description
	ip access-list	Defines an IP access list.

Platform	N/A
Description	

1.40 show ipv6 traffic-filter

	Use this command to display the IPv6 access list on the interface.	
	show ipv6 traffic-filter [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Defaults	-	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the IPv6 access list configured on the interface. If no interface is specified, the IPv6 access lists on all interfaces are displayed.	
Configuration Examples	FS# show ipv6 traffic-filter interface gigabitethernet 0/4 ipv6 access-group v6 in Applied On interface GigabitEthernet 0/4.	
Related Commands	Command	Description
	ipv6 access-list	Defines an IPv6 access list.
Platform	N/A	
Description		

1.41 show mac access-group

	Use this command to display the MAC access list on the interface.	
	show mac access-group [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Defaults	N/A	
Command mode	Privileged EXEC mode	

Usage Guide	Use this command to display the MAC access list configured on the interface. If no interface is specified, the MAC access lists on all interfaces are displayed.	
Configuration Examples	<pre>FS# show mac access-group interface gigabitethernet 0/3 mac access-group mm in Applied On interface GigabitEthernet 0/3.</pre>	
Related Commands	Command	Description
	mac access-list	Defines a MAC access list.
Platform Description	N/A	

1.42 show redirect interface

	Use this command to display the access redirection configuration.	
	show redirect [interface interface-name]	
Parameter Description	Parameter	Description
	interface interface-name	Interface name
Defaults	N/A	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the access redirection configuration on the interface. If no interface is specified, the access redirection configuration on all interfaces is displayed.	
Configuration Examples	The following example displays the access redirection configuration on interface GigabitEthernet 0/3. <pre>FS #show redirect interface gigabitEthernet 0/3 acl redirect configuration on interface gigabitEthernet 0/3 redirect destination interface gigabitEthernet 0/3 acl 1 in</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.43 svi router-acls enable

	Use this command to enable the SVI filter only for the Layer3 packets. Use the no form of this command to disable this function.	
	svi router-acls enable	
	no svi router-acls enable	
Parameter Description	Parameter	Description
	N/A	N/A.
Defaults	The SVI filter takes effect for both Layer2 and Layer3 packets by default.	
Command mode	Global configuration mode	
Usage Guide	Use this command to make the SVI filter take effect only for the Layer3 packets,	
Configuration Examples	The following example enables the SVI filter only for the Layer3 packets. <pre>FS(config)#svi router-acls enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2 QoS Commands

2.1 class

	Use this command to add reference to an existing class map. Use the no form of this command to remove the class from the policy map.	
	class <i>class-map-name</i>	
	no class <i>class-map-name</i>	
Parameter	Parameter	Description
Description	<i>class-map-name</i>	Reference to a class map.
Defaults	The function is disabled by default.	
Command Mode	Policy configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example adds reference to the class map named cmap1. <pre> FS(config)# class-map cmap1 FS(config-cmap)# match ip dscp 5 FS(config-cmap)# exit FS(config)# policy-map pmap1 FS(config-pmap)# class cmap1 FS(config-pmap-c)# end </pre>	
Related Commands	Command	Description
	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]]	Displays the policy map.
Platform Description	N/A	

2.2 class map

	Use this command to create a class map and enter class-map configuration mode. Use the no or default form of this command to remove a class map.

	class-map <i>class-map-name</i>	
	no class-map <i>class-map-name</i>	
	default class-map <i>class-map-name</i>	
Parameter	Parameter	Description
Description	<i>class-map-name</i>	Class map name. The class map name can be a maximum of 31 characters.
Defaults	None	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example creates a class map named cm_acl to match an access list named me. <pre>FS(config)# mac access-list extended me FS(config-ext-macl)# permit host 1111.2222.3333 any FS(config-ext-macl)# exit FS(config)# class-map cm_acl FS(config-cmap)# match access-group me FS(config-cmap)# exit</pre> The following example creates a class map named cm_dscp to match DHCP 8, 16 and 24. <pre>FS(config)# class-map cm_dscp FS(config-cmap)# match ip dscp 8 16 24 FS(config-cmap)# exit</pre>	
Related	Command	Description
Commands	show class-map [<i>class-map-name</i>]	Displays the class map.
Platform Description	N/A	

2.3 drr-queue bandwidth

	Use this command to set the DRR queue weight ratio. Use the no or default form of this command to restore the default setting.

	drr-queue bandwidth <i>weight1...weight8</i>	
	no drr-queue bandwidth	
	default drr-queue bandwidth	
Parameter	Parameter	Description
Description	<i>weight1...weight8</i>	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15.
Defaults	The default queue weight ratio is 1:1:1:1:1:1:1:1.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example configures the DRR queue weight ratio to 1:1:1:2:2:4:6:8. <pre>FS(config)# drr-queue bandwidth 1:1:1:2:2:4:6:8</pre>	
Related Commands	Command	Description
	show mls qos queuing	Displays information about the queue.
Platform Description	N/A	

2.4 match

	Use this command to define a match criteria in class map configuration mode. Use the no form of this command to remove the match criteria.	
	match { access-group <i>access_list</i> ip { dscp <i>dscp-vlaue-list</i> precedence <i>pre-vlaue-list</i> } }	
	no match { access-group <i>access_list</i> ip { dscp <i>dscp-vlaue-list</i> precedence <i>pre-vlaue-list</i> } }	
Parameter	Parameter	Description
Description	access-group <i>access_list</i>	Identifies a numbered or named access list as the match criteria.
	ip dscp <i>dscp-vlaue-list</i>	Identifies DSCP values as the match criteria. Multiple DSCP can be configured. The range is from 0 to 63.
	ip precedence <i>pre-vlaue-list</i>	Identifies IP precedence values as the match criteria. Multiple IP precedence can be configured. The range is from 0 to 7.
Defaults	None	

Command Mode	Class map configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example creates a class map named cmap1 to match DSCP 20, 22, 24 and 30. <pre>FS(config)# class-map cmap1 FS(config-cmap)# match ip dscp 20 22 24 30</pre>	
Related Commands	Command	Description
	show class-map [<i>class-map-name</i>]	Displays the class map.
Platform Description	N/A	

2.5 mls qos cos

	Use this command to configure the CoS value of an interface. Use the no form of this command to restore the default setting.	
	mls qos cos <i>default-cos</i>	
	no mls qos cos	
Parameter Description	Parameter	Description
	<i>default-cos</i>	CoS value of the interface. The range is from 0 to 7.
Defaults	The default CoS value is 0.	
Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the default CoS value to 7. <pre>FS(config)# interface gigabitethernet 1/1 FS(config-if)# mls qos cos 7</pre>	
Related Commands	Command	Description
	show mls qos interface <i>interface-id</i>	Displays information of the specified interface.
Platform Description	N/A	

2.6 mls qos map cos-dscp

	Use this command to map the CoS value to the DSCP value. Use the no or default form of this command to restore the default CoS-DSCP mapping.	
	mls qos map cos-dscp <i>dscp1...dscp8</i>	
	no mls qos map cos-dscp	
	default mls qos map cos-dscp	
Parameter	Parameter	Description
Description	<i>dscp1...dscp8</i>	Specifies the DSCP value. The range is from 0 to 63.
Defaults	By default, the CoS 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	FS(config)# mls qos map cos-dscp 8 10 16 18 24 26 32 34	
Related Commands	Command	Description
	show mls qos maps cos-dscp	Displays the CoS-DSCP mapping.
Platform Description	N/A	

2.7 mls qos map dscp-cos

	Use this command to map the DSCP value to the CoS value. Use the no or default form of this command to restore the default DSCP-CoS mapping.							
	mls qos map dscp-cos <i>dscp-list to cos</i>							
	no mls qos map dscp-cos							
	default mls qos map dscp-cos							
Parameter Description	Parameter		Description					
	<i>dscp-list</i>		DSCP list. The range is from 0 to 63.					
	<i>cos</i>		CoS value. The range is from 0 to 7.					
Defaults	The default DSCP-CoS mapping is listed below:							
	DSCP 0-7	DSCP 8-15	DSCP 16-23	DSCP 24-31	DSCP 32-39	DSCP 40-47	DSCP 48-55	DSCP 56-63
	CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7

Command Mode	Global configuration mode.					
Usage Guide	N/A					
Configuration Examples	FS(config)# mls qos map dscp-cos 8 10 16 18 to 0					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show mls qos maps dscp-cos</td><td>Displays the DSCP-CoS mapping.</td></tr></table>	Command	Description	show mls qos maps dscp-cos	Displays the DSCP-CoS mapping.	
Command	Description					
show mls qos maps dscp-cos	Displays the DSCP-CoS mapping.					
Platform Description	N/A					

2.8 mls qos map ip-precedence-dscp

	Use this command to map the IP precedence to the DSCP value. Use the no or default form of this command to restore the default IP-precedence to DSCP mapping.	
	mls qos map ip-precedence-dscp <i>dscp1 ... dscp8</i>	
	no mls qos map ip-precedence-dscp	
	default mls qos map ip-precedence-dscp	
Parameter	Parameter	Description
Description	<i>dscp1...dscp8</i>	DSCP list. The range is from 0 to 63.
Defaults	By default, the IP precedence 0, 1, 2, 3, 4, 5, 6, 7 is mapped to the DSCP 0, 8, 16, 24, 32, 40, 48, 56 respectively.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	FS(config)# mls qo map ip-prec -dscp 8 10 16 18 24 26 32 34	
Related Commands	Command	Description
	show mls qos maps ip-pre-dscp	Displays the IP-precedence to DSCP mapping.
Platform Description	N/A	

2.9 mls qos scheduler

	Use this command to configure the output queue scheduling. Use the no or default form of this command to restore the default scheduler.	
	mls qos scheduler [sp rr wrr drr]	
	no mls qos scheduler	
Parameter Description	Parameter	Description
	sp	Specifies the absolute priority scheduling.
	rr	Specifies the round-robin scheduling.
	wrr	Specifies the frame count weighted round-robin scheduling.
	drr	Specifies the frame length weighted round-robin scheduling.
Defaults	The default queue scheduling is wrr globally, no queue scheduling is configured on the interface.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example specifies the sp scheduling.	
	<pre>FS(config)# mls qos scheduler sp</pre>	
Related Commands	Command	Description
	show mls qos scheduler	Displays the output queue scheduling.
Platform Description	N/A	

2.10 mls qos trust

	Use this command to configure the trust mode on an interface. Use the no or default form of this command to restore the default setting.	
	mls qos trust { cos dscp ip-precedence }	
	no mls qos trust	
	default mls qos trust	
Parameter Description	Parameter	Description
	cos	Specifies the CoS trust mode.
	dscp	Specifies the DSCP trust mode.
	ip-precedence	Specifies the IP-PRE trust mode.
Defaults	No trust mode is configured by default.	

Command Mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the CoS trust mode. FS(config)# interface gigabitethernet 1/1 FS(config-if)# mls qos trust cos	
Related Commands	Command	Description
	show mls qos interface <i>interface-id</i>	Displays the specified interface configuration.
Platform Description	N/A	

2.11 police

	Use this command to configure traffic policing for a class map in a policy map. Use the no form of this command to remove traffic policing for the class map.	
	police <i>rate-bps burst-byte</i> [exceed-action { drop dscp <i>new-dscp</i> cos <i>new-cos</i> [none-tos] }]	
	no police	
Parameter Description	Parameter	Description
	<i>rate-bps</i>	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
	<i>burst-byte</i>	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.
	drop	Drops the packet. This is available only when the packet exceeds the bandwidth limit.
	dscp <i>new-dscp</i>	Modifies the DSCP value of the packet. This is available only when the packet exceeds bandwidth limit. The DSCP value range is from 0 to 63.
	cos <i>new-cos</i>	Modifies the CoS value of the packet. This is available only when the packet exceeds bandwidth limit. The CoS value range is from 0 to 7.
	none-tos	Modifies the CoS value only.
Defaults	No traffic policing is configured for the class map by default.	
Command Mode	Policy map class configuration mode	
Usage Guide	N/A	
Configuration	The following example configures traffic policing which modifies the DSCP value of the packet to 16 for class map	

Examples	"cm-acl" in policy map "pmap1". <pre>FS(config)# policy-map pmap1 FS(config-pmap)# class cm-acl FS(config-pmap-c)# police 102400 4096 exceed-action dscp 16</pre>	
Related		
Commands	Command	Description
	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]]	Displays the policy map configuration.
Platform	N/A	
Description		

2.12 policy map

	Use the following command to create a policy map and enter policy map configuration mode. Use the no or default form of this command to remove the specified policy map.	
	policy-map <i>policy-map-name</i>	
	no policy-map <i>policy-map-name</i>	
	default policy-map <i>policy-map-name</i>	
Parameter	Parameter	Description
Description	<i>policy-map-name</i>	Policy map name. The policy map name can be a maximum of 31 characters.
Defaults	No policy map is configured by default.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example creates policy map “po”, and then adds a reference to class map “cmap1”. Sets the rate limit value to 10 Mbps, the burst traffic limit value to 256 Kbps, and discard packets which exceed the limit. <pre>FS(config)# policy-map po FS(config-pmap)# class cmap1 FS(config-pmap-c)# police 10240 256 exceed-action drop</pre>	
Related Commands	Command	Description
	show policy-map [<i>policy-map-name</i> [class]]	Displays the policy map configuration.

	<code>class-map-name]]</code>	
Platform Description	N/A	

2.13 priority-queue

	Use this command to configure the output queue scheduling policy to SP. Use the no or default form of this command to restore the default queue scheduling policy.	
	priority-queue	
	no priority-queue	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The default output queue scheduling policy is WRR.	
Command Mode	Global configuration mode.	
Usage Guide	This command shares the same configuration with the mls qos scheduler sp . The show run command displays this configuration in the mls qos scheduler sp item instead of priority-queue .	
Configuration Examples	The following example configures the output queue scheduling policy to SP. FS(config)# priority-queue	
Related Commands	Command	Description
	show mls qos scheduler	Displays the output queue scheduling policy.
Platform Description	N/A	

2.14 priority-queue cos-map

	Use this command to configure the mapping between the CoS value and the queue ID. Use the no or default form of this command to restore the default CoS mapping to the queue.	
	priority-queue cos-map <i>qid cos0 [cos1 [cos2 [cos3 [cos4 [cos5 [cos6 [cos7]]]]]]]</i>	
	no priority-queue cos-map	
	default priority-queue cos-map	
Parameter Description	Parameter	Description
	<i>qid</i>	Queue ID. The range is from 1 to 8.
	<i>cos0 ... cos7</i>	CoS value. The range is from 0 to 7.

Defaults	The default mapping between the CoS value and the queue ID is listed below:							
	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7	Queue 8
	CoS 0	CoS 1	CoS 2	CoS 3	CoS 4	CoS 5	CoS 6	CoS 7
Command Mode	Global configuration mode.							
Usage Guide	N/A							
Configuration Examples	The following example maps the CoS 3, 5 to the output queue 1.							
	FS(config)#priority-queue cos-map 1 3 5							
Related Commands	Command			Description				
	show mls qos queuing			Displays the output queues.				
Platform Description	N/A							

2.15 qos mc-queue cos-map

	This command is used to configure the mapping between CoS values of multicast queues.	
	qos mc-queue cos-map <i>cos0-qid cos1-qid cos2-qid cos3-qid cos4-qid cos5-qid cos6-qid cos7-qid</i>	
	no qos mc-queue cos-map	
Parameter Description	Parameter	Description
	<i>cosN-qid</i>	Queue ID mapped by the packet whose CoS is N. The value of N ranges from 0 to 7, and queue ID ranges from 1 to 3.
Defaults	The default value is different from products.	
Command Mode	Global configuration mode	
Usage Guide	In the case of default configuration, the relevant trust mode must be enabled. For example, packets can enter the default mapped queue only when CoS is trusted.	
Configuration Examples	The following example sets the CoS 0, 1, 2, 3, 4, 5, 6, 7 to be mapped to the multicast queues 1 1 1 2 2 2 2 3 respectively. <pre>FS(config)# qos mc-queue cos-map 1 1 1 2 2 2 2 3</pre>	
Related Commands	Command	Description
	show qos mc-queue cos-map	This command is used to view the queue mapping.

Platform	N/A
Description	

2.16 qos queue

	Use this command to configure a minimum or maximum of the interface bandwidth to a queue. Use the no or default form of this command to remove the minimum or maximum of the interface bandwidth.	
	qos queue <i>queue-id</i> bandwidth { minimum maximum } <i>bandwidth</i>	
	no qos queue <i>queue-id</i> bandwidth { minimum maximum }	
	default qos queue <i>queue-id</i> bandwidth { minimum maximum }	
Parameter Description	Parameter	Description
	queue	Configure the minimum or maximum of the interface bandwidth to the queue on the device supporting both unicast and multicast queue bandwidth configuration.
	<i>queue-id</i>	Queue ID. The range is from 1 to 8.
	bandwidth { mini mum maximum } <i>bandwidth</i>	Bandwidth value. The value range depends on the specific product.
Defaults	No minimum or maximum of interface bandwidth to a queue is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	Support global configuration mode and interface configuration mode. Function that these two modes support is different.	
Configuration Examples	The following example configures the minimum interface bandwidth of queue 1 to 5 Mbps and the maximum to 10 Mbps; the minimum interface bandwidth of queue 2 to 1 Mbps and the maximum to 5 Mbps; <pre> FS(config)# interface gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth maximum 10240 FS(config-if-GigabitEthernet 0/1)# qos queue 1 bandwidth minimum 5120 FS(config-if-GigabitEthernet 0/1)# qos queue 2 bandwidth minimum 2048 </pre>	
Related Commands	Command	Description
	show qos bandwidth [interfaces <i>interface-id</i>]	Displays the interface bandwidth of the queue.
Platform Description	N/A	

2.17 queueing wred

	Use this command to enable the WRED (Weighted Random Early Detection) function. Use the no or default form of this command to disable the WRED function.	
	queueing wred	
	no queueing wred	
	default queueing wred	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	WRED is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables WRED. <pre>FS(config)# queueing wred</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.18 rate-limit

	Use this command to configure rate limiting on the interface. Use the no or default form of this command to remove rate limiting from the interface.	
	rate-limit { input output } bps burst-size	
	no rate-limit { input output }	
	default rate-limit { input output }	
Parameter	Parameter	Description
Description	input	Configures input rate limiting.
	output	Configures output rate limiting.
	<i>bps</i>	Bandwidth limit value per second (The unit is KBits). This value depends on the specific product.
	<i>burst-size</i>	Burst traffic limit value (The unit is KBytes). This value depends on the specific product.

Defaults	Rate limiting is not configured by default.					
Command Mode	Interface configuration mode.					
Usage Guide	N/A					
Configuration Examples	The following example configures the rate limit value to 10 Mbps, and the burst traffic limit value to 256 Kbps. <pre>FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)# rate-limit input 10240 256</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show mls qos rate-limit [interface <i>interface-id</i>]</td><td>Displays the rate limiting configuration of the interface.</td></tr></table>	Command	Description	show mls qos rate-limit [interface <i>interface-id</i>]	Displays the rate limiting configuration of the interface.	
Command	Description					
show mls qos rate-limit [interface <i>interface-id</i>]	Displays the rate limiting configuration of the interface.					
Platform Description	N/A					

2.19 service-policy

	Use this command to apply the policy map to the interface, the virtual group or globally. Use the no or default form of this command to remove the policy map.	
	service-policy { input output } <i>policy-map-name</i>	
	no service-policy { input output } <i>policy-map-name</i>	
	default service-policy { input output } <i>policy-map-name</i>	
Parameter Description	Parameter	Description
	<i>policy-map-name</i>	Policy map name
	input	Applies the policy map to the input direction.
	output	Applies the policy map to the output direction.
Defaults	No policy map is configured on the interface or virtual group by default.	
Command Mode	Interface configuration mode, and virtual group configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example applies policy map “po” to the input direction of interface GigabitEthernet 1/3. FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)# service-policy input po	

	The following example applies policy map “po” to the output direction of virtual group 3. <pre>FS(config)# virtual-group 3 FS(config-VirtualGroup)# service-policy output po</pre>	
Related Commands	Command	Description
	show mls qos interface policers	Displays the policy map configuration on the interface.
	show mls qos virtual-group policers	Displays the policy map configuration on the virtual group.
Platform Description	N/A	

2.20 set

	Use this command to configure the CoS, DSCP or VID value for the traffic. Use the no form of this command to remove the CoS, DSCP or VID value from the traffic.	
	set { ip dscp new-dscp cos new-cos [none-tos] vid new-vid }	
	no set { ip dscp cos vid }	
Parameter Description	Parameter	Description
	ip dscp new-dscp	Configures the DSCP value for the traffic. The range is from 0 to 63.
	cos new-cos	Configures the CoS value for the traffic. The range is from 0 to 7.
	none-tos	Configures the CoS value only.
	vid new-vid	Configures the VID value for the traffic. The range is from 1 to 4094.
Defaults	No CoS, DSCP or VID value is configured for the traffic in policy map class mode.	
Command Mode	Policy map class configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example creates policy map “pmap1”, and adds a reference to class map “cmap1”. <pre>FS(config)# policy-map pmap1 FS(config-pmap)# class cmap1</pre>	
	The following example modifies the CoS value of the traffic to 3. <pre>FS(config-pmap-c)# set cos 3</pre>	
Related Commands	Command	Description
	show	Displays the policy map configuration on the interface.

	policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]]	
Platform	N/A	
Description		

2.21 show class-map

	Use this command to display the class map.	
	show class-map [<i>class-map-name</i>]	
Parameter	Parameter	Description
Description	<i>class-map-name</i>	Class map name.
Defaults	None	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays all class maps.	
	<pre>FS# show class-map Class Map cmap1 Match ip dscp 20 40 Class Map cmap2 Match access-group 110</pre>	
	The fields in the output of this command are described in the following table.	
	Field	Description
	Class Map	Indicates the class map name.
Match	Indicates the matched rule.	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.22 show mls qos interface

	Use this command to display the QoS configuration of the interface.																
	show mls qos interface [<i>interface-id</i>] [policers]																
Parameter Description	Parameter	Description															
	<i>interface-id</i>	Interface name															
	policers	Displays the traffic policing configured on the interface.															
Defaults	None																
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.																
Usage Guide	N/A																
Configuration Examples	The following example displays the QoS configuration of interface GigabitEthernt 1/3.																
	FS# show mls qos interface gigabitethernet 1/3																
	Interface: GigabitEthernet 1/3																
	Ratelimit input: 10240 256																
	Ratelimit output: 51200 4096																
	Attached input policy-map: pmap1																
	Attached output policy-map:																
	Default trust: dscp																
	Default cos: 3																
	The fields in the output of this command are described in the following table.																
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface</td><td>Indicates the interface name.</td></tr><tr><td>Ratelimit input</td><td>Indicates the input rate limit value .</td></tr><tr><td>Ratelimit output</td><td>Indicates the output rate limit value .</td></tr><tr><td>Attached input policy-map</td><td>Indicates the input policy map .</td></tr><tr><td>Attached output policy-map</td><td>Indicates the output policy map.</td></tr><tr><td>Default trust</td><td>Indicates the trust mode of the interface.</td></tr><tr><td>Default cos</td><td>Indicates the default CoS value.</td></tr></table>	Field	Description	Interface	Indicates the interface name.	Ratelimit input	Indicates the input rate limit value .	Ratelimit output	Indicates the output rate limit value .	Attached input policy-map	Indicates the input policy map .	Attached output policy-map	Indicates the output policy map.	Default trust	Indicates the trust mode of the interface.	Default cos	Indicates the default CoS value.
Field	Description																
Interface	Indicates the interface name.																
Ratelimit input	Indicates the input rate limit value .																
Ratelimit output	Indicates the output rate limit value .																
Attached input policy-map	Indicates the input policy map .																
Attached output policy-map	Indicates the output policy map.																
Default trust	Indicates the trust mode of the interface.																
Default cos	Indicates the default CoS value.																
	The following example displays the QoS configuration of all interfaces.																
	FS# show mls qos interface policers																
	Interface: GigabitEthernet 0/1																
	Attached input policy-map: pmap1																
	Attached output policy-map: pmap1																

	Interface: GigabitEthernet 0/2	
	Attached input policy-map: p1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.23 show mls qos maps

	Use this command to display DSCP-CoS mapping, CoS-DSCP mapping and IP-PRE-DSCP mapping.	
	show mls qos maps [cos-dscp dscp-cos ip-prec-dscp]	
Parameter Description	Parameter	Description
	cos-dscp	Displays the CoS-DSCP mapping.
	dscp-cos	Displays the DSCP-CoS mapping.
	ip-prec-dscp	Displays the IP-PRE-DSCP mapping..
Defaults	None	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the CoS-DSCP mapping. <pre> FS# show mls qos maps cos-dscp cos dscp ----- 0 0 1 8 2 16 3 24 4 32 5 40 6 48 7 56 </pre> The fields in the output of this command are described in the following table.	

Field	Description
cos	Indicates the CoS value.
dscp	Indicates the DSCP value mapped .

The following example displays the DSCP- CoS mapping.

FS# show mls qos maps dscp-cos

```

dscp cos      dscp cos      dscp cos      dscp cos
-----
 0   0         1   0         2   0         3   0
 4   0         5   0         6   0         7   0
 8   1         9   1        10   1        11   1
12   1        13   1        14   1        15   1
16   2        17   2        18   2        19   2
20   2        21   2        22   2        23   2
24   3        25   3        26   3        27   3
28   3        29   3        30   3        31   3
32   4        33   4        34   4        35   4
36   4        37   4        38   4        39   4
40   5        41   5        42   5        43   5
44   5        45   5        46   5        47   5
48   6        49   6        50   6        51   6
52   6        53   6        54   6        55   6
56   7        57   7        58   7        59   7
60   7        61   7        62   7        63   7

```

The fields in the output of this command are described in the following table.

Field	Description
dscp	Indicates the DSCP value.
cos	Indicates the CoS value mapped .

The following example displays the IP-PRE-DSCP mapping.

FS# show mls qos maps ip-prec-dscp

ip-precedence dscp

	----- 0 0 1 8 2 16 3 24 4 32 5 40 6 48 7 56							
	The fields in the output of this command are described in the following table.							
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>ip-precedence</td><td>Indicates the IP-PRE value.</td></tr><tr><td>dscp</td><td>Indicates the DSCP value mapped .</td></tr></table>	Field	Description	ip-precedence	Indicates the IP-PRE value.	dscp	Indicates the DSCP value mapped .	
Field	Description							
ip-precedence	Indicates the IP-PRE value.							
dscp	Indicates the DSCP value mapped .							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A			
Command	Description							
N/A	N/A							
Platform Description	N/A							

2.24 show mls qos queueing

	Use this command to display the QoS queuing configuration.	
	show mls qos queueing [interface <i>interface-id</i>]	
Parameter	Parameter	Description
Description	interface <i>interface-id</i>	ID of interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the QoS queuing configuration. FS# show mls qos queueing Cos-queue map: cos qid --- ---	

0 1

1 2

2 3

3 4

4 5

5 6

6 7

7 8

wrr bandwidth weights:

qid weights

1 1

2 2

3 3

4 4

5 5

6 6

7 7

8 8

drp bandwidth weights:

qid weights

1 3

2 3

3 3

4 3

5 3

6 3

7 3

8 3

wfq bandwidth weights:

```
qid weights
```

```
-----
```

```
1    3
```

```
2    4
```

```
3    5
```

```
4    6
```

```
5    7
```

```
6    8
```

```
7    9
```

```
8   10
```

```
Interface: GigabitEthernet 0/1
```

```
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
```

```
Drr queue bandwidth: 1 1 2 2 2 2 4 4
```

```
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

The fields in the output of this command are described in the following table.

Field	Description
Cos-queue map	Indicates the mapping between the CoS value and the queue ID.
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.
cos	Indicates the CoS value.
qid	Indicates the queue ID.
Weights	Indicates the weight value
Interface	Interface name
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.

```
FS# show mls qos queueing interface gigabitEthernet 0/1
```

```
Interface: GigabitEthernet 0/1
```

```
Wrr queue bandwidth: 1 1 1 1 2 2 2 2
```

```
Drr queue bandwidth: 1 1 2 2 2 2 4 4
```

```
Wfq queue bandwidth: 1 1 2 2 4 4 4 4
```

Interface	Interface name
wrr bandwidth weights	Indicates the WRR queue weight.
drr bandwidth weights	Indicates the DRR queue weight.
wfq bandwidth weights	Indicates the WFQ queue weight.

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.25 show mls qos rate-limit

	Use this command to display the rate limiting configuration of the interface.									
	show mls qos rate-limit [interface <i>interface-id</i>]									
Parameter	Parameter	Description								
Description	<i>interface-id</i>	Interface name								
Defaults	N/A									
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.									
Usage Guide	N/A									
Configuration Examples	The following example displays the rate limiting configuration of all interfaces. <pre>FS# show mls qos rate-limit Interface: GigabitEthernet 0/1 rate limit input Kbps = 10240 burst = 256 Interface: GigabitEthernet 0/3 rate limit output Kbps = 102400 burst = 4096</pre> The fields in the output of this command are described in the following table. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface</td><td>Indicates the interface name.</td></tr><tr><td>rate limit input Kbps = x burst = y</td><td>Indicates the input rate limit value, and the input burst traffic limit value.</td></tr><tr><td>rate limit output Kbps = x burst = y</td><td>Indicates the output rate limit value, and the output burst traffic limit value.</td></tr></table>		Field	Description	Interface	Indicates the interface name.	rate limit input Kbps = x burst = y	Indicates the input rate limit value, and the input burst traffic limit value.	rate limit output Kbps = x burst = y	Indicates the output rate limit value, and the output burst traffic limit value.
Field	Description									
Interface	Indicates the interface name.									
rate limit input Kbps = x burst = y	Indicates the input rate limit value, and the input burst traffic limit value.									
rate limit output Kbps = x burst = y	Indicates the output rate limit value, and the output burst traffic limit value.									
Related Commands	Command	Description								
	N/A	N/A								
Platform Description	N/A									

2.26 show mls qos scheduler

	Use this command to display the queue scheduling policy.	
	show mls qos scheduler [interface <i>interface-id</i>]	
Parameter	Parameter	Description
Description	interface <i>interface-id</i>	Interface name
Defaults	None	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the queue scheduling policy.	
	FS# show mls qos scheduler	
	Global Multi-Layer Switching scheduling	
	Weighted Round Robin	
	Interface GigabitEthernet 0/1 Multi-Layer Switching scheduling:	
	Deficit Round Robin	
	The fields in the output of this command are described in the following table.	
	Field	Description
	Weighted Round Robin	Indicates that the queue scheduling policy is WRR. The other queue scheduling policies are listed as follows: SP: Strict Priority RR: Round Robin DRR: Deficit Round Robin WFQ: Weighted Fair Queue
	Interface	Interface name
	Deficit Round Robin	The queue scheduling is DRR
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.27 show mls qos virtual-group

	Use this command to display the policy map configuration on the virtual group.	
	show mls qos virtual-group [<i>virtual-group-number</i> policers]	
Parameter Description	Parameter	Description
	<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.
	policers	Displays the policy map configuration on all virtual groups.
Defaults	None	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the policy map configuration on all virtual groups.	
	FS# show mls qos virtual-group policers Virtual-group: 1 Attached input policy-map: pmap1 Virtual-group: 20 Attached output policy-map: pmap2	
	The fields in the output of this command are described in the following table.	
	Field	Description
	Virtual-group	Indicates the virtual group number.
	Attached input policy-map	Indicates the policy map applied on the input virtual group.
	Attached output policy-map	Indicates the policy map applied on the output virtual group.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.28 show policy-map

	Use this command to display policy maps.
	show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]]

Parameter	Parameter	Description										
Description	policy-map-name	Policy map name										
	class-map-name	Class map name										
Defaults	None											
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.											
Usage Guide	N/A											
Configuration Examples	The following example displays configuration of policy map “pmap1”.											
	<pre>FS# show policy-map pmap1 Policy Map pmap1 Class cmap1 set ip dscp 16 Class cmap2 police 10240 256 exceed-action dscp 8 Class cmap3 police 512000 4096 exceed-action drop</pre>											
	The fields in the output of this command are described in the following table.											
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Policy Map</td><td>Indicates the policy map name.</td></tr><tr><td>Class</td><td>Indicates the class map name.</td></tr><tr><td>set</td><td>Indicates that the DSCP value is modified in this example.</td></tr><tr><td>police</td><td>Indicates bandwidth limit configuration and the action policy for the violated packets.</td></tr></table>		Field	Description	Policy Map	Indicates the policy map name.	Class	Indicates the class map name.	set	Indicates that the DSCP value is modified in this example.	police	Indicates bandwidth limit configuration and the action policy for the violated packets.
Field	Description											
Policy Map	Indicates the policy map name.											
Class	Indicates the class map name.											
set	Indicates that the DSCP value is modified in this example.											
police	Indicates bandwidth limit configuration and the action policy for the violated packets.											
	The following example displays the action policy for the traffic of class map “cmap1” in policy map “pmap1” .											
	<pre>FS#show policy-map pmap1 class cmap1 Class cmap1 set ip dscp 16</pre>											

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.29 show qos bandwidth

	Use this command to display the bandwidth configuration.				
	show qos bandwidth [interfaces <i>interface-id</i>]				
Parameter Description	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td><i>interface-id</i></td><td>Interface name</td></tr> </table>	Parameter	Description	<i>interface-id</i>	Interface name
Parameter	Description				
<i>interface-id</i>	Interface name				
Defaults	None				
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.				
Usage Guide	N/A				
Configuration Examples	The following example displays the bandwidth configuration of interface GigabitEthernet 0/1. (Taking the device supporting the bandwidth configuration of the unicast queue or the multicast queue for example.) <pre>FS# show qos bandwidth interface gigabitEthernet 0/1</pre> Interface: GigabitEthernet 0/1 <pre>----- uc-queue-id minimum-bandwidth maximum-bandwidth ----- 1 5120 10240 2 0 0 3 0 0 4 0 0 5 0 0 6 0 0 7 0 0 8 0 0 ----- Total ucast-queue minimum-bandwidth: 5120</pre>				

Total ucast-queue maximum-bandwidth: 10240

Interface: GigabitEthernet 0/1

mc-queue-id | minimum-bandwidth | maximum-bandwidth

1	1024	5120
2	0	0
3	0	0
4	0	2048

Total mcast-queue minimum-bandwidth: 1024

Total mcast-queue maximum-bandwidth: 5120

The fields in the output of this command are described in the following table.

Field	Description
Interface	Indicates the interface name.
queue-id	Indicates the queue ID.
uc-queue-id	Indicates the unicast queue ID.
mc-queue-id	Indicates the multicast queue ID.
minimum-bandwidth	Indicates the minimum bandwidth configuration. The unit is Kbps.
maximum-bandwidth	Indicates the maximum bandwidth configuration. The unit is Kbps.
Total queue minimum-bandwidth Total queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when both unicast and multicast queues are displayed.
Total ucast-queue minimum-bandwidth Total ucast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only unicast queue is displayed.
Total mcast-queue minimum-bandwidth Total mcast-queue maximum-bandwidth	Indicates the total bandwidth of minimum and maximum when only multicast queue is displayed.

Related

Commands

Command	Description
N/A	N/A

Platform

Description

N/A

2.30 show qos mc-queue cos-map

	This command is used to display the mapping between multicast queues and priorities.	
	show qos mc-queue cos-map	
Parameter	Parameter	Description
Description	-	-
Defaults	-	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	-	
Configuration Examples	The following example displays the mapping between multicast queues and priorities <pre> FS# show qos mc-queue cos-map Cos to multicast queue map: Cos Queue id ----- 0 1 1 1 2 1 3 1 4 2 5 2 6 2 7 3 </pre>	
Related Commands	Command	Description
	Cos	Cos value
	Queue id	Queue ID of Cos
Platform Description	N/A	

2.31 show qos mc-queue scheduler

	This command is used to display the scheduling algorithm for multicast queues.	
	show qos mc-queue scheduler [interfaces interface-id]	
Parameter	Parameter	Description
Description	interfaces interface-id	Interface to be displayed.

Defaults	-	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	-	
Configuration Examples	The following example displays the scheduling algorithm for multicast queues.	
	<pre>FS# show qos mc-queue scheduler Multicast queue scheduler: Interface GigabitEthernet 0/0 : Strict Priority Interface GigabitEthernet 0/1 : Strict Priority Interface GigabitEthernet 0/2 : Weighted Round Robin Queue id Weight ----- 1 1 2 2 3 4</pre>	
Related Commands	Command	Description
	qos mc-queue scheduler mode {sp wrr}	This command is used to configure the scheduling algorithm for multicast queues.
	qos mc-queue scheduler weight weight1 weight2 weight3	This command is used to configure the WRR algorithm weight for multicast queues.
Platform Description	N/A	

2.32 show queueing wred interface

	Use this command to display WRED settings on the interface.
	show queueing wred interface <i>interface-id</i>

Parameter Description	Parameter	Description						
	<i>interface-id</i>	Interface name						
Defaults	None							
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode.							
Usage Guide	N/A							
Configuration Examples	The following example displays the WRED settings on interface GigabitEthernet 0/1. FS#show queueing wred interface gigabitEthernet 0/1 ----- qid min_1 prob_1 min_2 prob_2 ----- 1 100 60 80 80 2 100 60 80 80 3 100 60 80 80 4 100 60 80 80 5 100 60 80 80 6 100 60 80 80 7 100 60 80 80 8 100 60 80 80 ----- cos qid threshold_id ----- 0 1 1 1 2 1 2 3 1 3 4 1 4 5 1 5 6 1 6 7 1 7 8 1 The fields in the output of this command are described in the following table. <table><tr><th>Field</th><th>Description</th></tr><tr><td>qid</td><td>Indicates the queue ID.</td></tr><tr><td>cos qid threshold_id</td><td>Indicates the mapping of CoS value, queue ID and threshold number.</td></tr></table>		Field	Description	qid	Indicates the queue ID.	cos qid threshold_id	Indicates the mapping of CoS value, queue ID and threshold number.
Field	Description							
qid	Indicates the queue ID.							
cos qid threshold_id	Indicates the mapping of CoS value, queue ID and threshold number.							

Related Commands	Command	Description
	N/A.	N/A.
Platform Description	N/A.	

2.33 show virtual-group

	Use this command to display the member port in the virtual group.	
	show virtual-group [<i>virtual-group-number</i> summary]	
Parameter Description	Parameter	Description
	<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.
	summary	Displays the member port in all virtual groups.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the member port in all virtual groups.	
	<pre> FS# show virtual-group summary virtual-group member ----- 1 Gi0/1 Gi0/2 2 Gi0/0 </pre>	
	The fields in the output of this command are described in the following table.	
	Field	Description
	virtual-group	Indicates the virtual group number.
	member	Indicates the member port in the virtual group.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.34 virtual-group

	Use this command to create a virtual group in global configuration mode. Use this command to configure add an interface to a virtual group in interface configuration mode. Use the no or default form of this command to remove a virtual group in global configuration mode. Use the no or default form of this command to remove an interface from a virtual group in interface configuration mode.	
	virtual-group <i>virtual-group-number</i>	
	no virtual-group <i>virtual-group-number</i>	
	default virtual-group <i>virtual-group-number</i>	
Parameter Description	Parameter	Description
	<i>virtual-group-number</i>	Virtual group number. The range is from 1 to 128.
Defaults	No virtual group is configured, or no interface is added to a virtual group, by default.	
Command Mode	Interface configuration mode, global configuration mode.	
Usage Guide	The member port added to the virtual group must be a physical port or an aggregate port member. The member ports of a virtual group must be on the same module of a chassis switch or on the same box switch.	
Configuration Examples	The following example sets the interface gigabitEthernet 1/3 as the member of virtual group 3: <pre>FS(config)# interface gigabitEthernet 1/3 FS(config-if)# virtual-group 3</pre>	
Related Commands	Command	Description
	show virtual-group [<i>virtual-group-number</i> summary]	Displays the virtual group configuration.
Platform Description	N/A	

2.35 wrr-queue bandwidth

	Use this command to set the WRR weight ratio. Use the no or default form of this command to restore the default setting.
	wrr-queue bandwidth <i>weight1 ... weight8</i>
	no wrr-queue bandwidth
	default wrr-queue bandwidth

Parameter	Parameter	Description
Description	<i>weight1...weight8</i>	8 queue weights. The default queue weight ratio is 1:1:1:1:1:1:1:1. For the products supporting the SP scheduling policy, the weight range is from 0 to 15. For the products not supporting the SP scheduling policy, the weight range is from 1 to 15.
Defaults	The default queue weight ratio is 1:1:1:1:1:1:1:1.	
Command Mode	Global/Interface configuration mode	
Usage Guide	If the weight value is 0, the SP scheduling policy is applied.	
Configuration Examples	The following example configures the WRR queue weight ratio to 1:1:1:1:2:2:4:8. <pre>FS(config)# wrr-queue bandwidth 1 1 1 1 2 2 4 8</pre>	
Related Commands	Command	Description
	show mls qos queuing	Displays the QoS queuing configuration.
Platform Description	N/A	

2.36 wrr-queue cos-map

	Use this command to map the CoS value to a threshold for a specified queue. Use the no or default form of this command to restore the default settings	
	wrr-queue cos-map <i>threshold_id</i> <i>cos1</i> [<i>cos2</i> [<i>cos3</i> [<i>cos4</i> [<i>cos5</i> [<i>cos6</i> [<i>cos7</i> [<i>cos8</i>]]]]]]]	
	no wrr-queue cos-map <i>threshold_id</i>	
	default wrr-queue cos-map <i>threshold_id</i>	
Parameter Description	Parameter	Description
	<i>threshold_id</i>	Threshold number. The range is from 1 to 2. Up to two threshold values can be configured.
	<i>cos_N</i>	CoS value. The range is from 0 to 7. Up to 8 CoS values can be configured.
Defaults	All CoS values are mapped to the threshold 1.	
Command mode	Interface configuration mode.	
Usage Guide	DSCP-threshold mapping can be enabled by mapping DSCP-CoS to CoS-threshold.	

	When all CoS values are mapped to one threshold on the interface, it changes the enabled WRED to RED.	
Configuration Examples	The following example enters the interface GigabitEthernet 1/3 to map CoS 1, 2 to threshold 2. FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)#wrr-queue cos-map 2 1 6	
Related Commands	Command	Description
	show queueing wred interface <i>interface-id</i>	Displays the WRED configuration on the interface.
Platform Description	N/A.	

2.37 wrr-queue random-detect min-threshold

	Use this command to configure the minimum WRED drop threshold. Use the no or default form of this command to restore the default WRED drop threshold.	
	wrr-queue random-detect min-threshold <i>queue_id</i> <i>thr1</i> [<i>thr2</i>]	
	no wrr-queue random-detect min-threshold <i>queue_id</i>	
	default wrr-queue random-detect min-threshold <i>queue_id</i>	
Parameter Description	Parameter	Description
	<i>queue_id</i>	Queue ID.
	<i>thrN</i>	Up to two threshold values can be configured. The threshold value range is from 1 to 100.
Defaults	Two threshold values are configured, and the default threshold values are 100 and 80.	
Command mode	Interface configuration mode.	
Usage Guide	Because the maximum value of the configuration range is equal to the current higher threshold, you need to pay attention to the setting of the higher threshold when configuring the lower threshold.	
Configuration Examples	The following example configures the low WRED drop thresholds to 60 and 70 for queue 1. FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)# wrr-queue random-detect min-threshold 1 60 70	

Related Commands	Command	Description
	show queueing wred interface <i>interface-id</i>	Displays the WRED configuration on the interface.
Platform Description	N/A.	

2.38 wrr-queue random-detect probability

	Use this command to configure the WRED packet drop probability. Use the no or default form of this command to restore the WRED packet drop probability.	
	wrr-queue random-detect probability <i>queue_id</i> <i>prob1</i> [<i>prob2</i>]	
	no wrr-queue random-detect probability <i>queue_id</i>	
	default wrr-queue random-detect probability <i>queue_id</i>	
Parameter Description	Parameter	Description
	<i>queue_id</i>	Queue ID.
	<i>proN</i>	Up to two probability values can be configured. The threshold value range is from 1 to 100.
Defaults	Two packet drop probability values are configured, and the default probability values are 100 and 80.	
Command mode	Interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the WRED packet drop values to 50 and 70 for queue 1. <pre>FS(config)# interface gigabitethernet 1/3 FS(config-if-GigabitEthernet 1/3)# wrr-queue random-detect probability 1 50 70</pre>	
Related Commands	Command	Description
	show queueing wred interface <i>interface-id</i>	Displays the WRED configuration on the interface.
Platform Description	N/A.	

3 MMU Commands

3.1 mmu buffer-mode

	Use this command to configure global buffer mode. mmu buffer-mode { normal burst-enhance qos-enhance flowctrl-enhance }	
	Use the no form of this command to restore the default setting. no mmu buffer-mode	
Parameter Description	Parameter	Description
	normal	Normal buffer mode
	burst-enhance	Burst enhancement
	qos-enhance	QoS enhancement
	flowctrl-enhance	Flow control enhancement
Defaults	The default buffer mode varies from product.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example configures the normal buffer mode. FS# mmu buffer-mode normal	
Platform Description	N/A	

3.2 clear queue-buffer peaked

	Use this command to clear the historical peak value of the queue buffer. clear queue-buffer peaked	
Parameter Description	Parameter	Description
	N/A	
Command Mode	Privileged EXEC mode	

Default Level	14
Usage Guide	N/A
Configuration Examples	The following example clears the historical peak value of the buffer. <pre>FS# clear queue-buffer peaked FS#</pre>
Platform Description	N/A

3.3 clear queue-counters

	Use this command to clear queue statistics. clear queue-counter [interface <i>interface_id</i>]	
Parameter Description	Parameter	Description
	<i>interface_id</i>	Port Number
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example clears all queue statistics. <pre>FS# clear queue-counter FS#</pre> The following example clears queue statistics of an interface. <pre>FS# clear queue-counter Interface TenGigabitEthernet 1/9 FS#</pre>	
Platform Description	N/A	

3.4 mmu usage-warn-limit

	Use this command to configure the usage warning threshold. mmu usage-warn-limit [{ unicast } { <i>queue-id1</i> [<i>queue-id2</i> [<i>queue-idN</i>]]} set <i>value</i>	
	Use the no form of this command to restore the default setting. no mmu usage-warn-limit	
Parameter Description	Parameter	Description
	unicast	Performs buffer management on the output unicast queue.
	<i>queue-idN</i>	Queue ID
	<i>priority-idN</i>	Priority group ID
	<i>value</i>	Usage warning threshold.
Defaults	The default threshold is 0.	
Command Mode	Global configuration mode/Interface configuration mode	
Default Level	14	
Usage Guide	If the buffer usage for the port group exceeds the global threshold, a warning log is printed. If the buffer usage for the queue exceeds the queue threshold, a warning log is printed. To avoid producing excessive logs, the warning log for a port group/queue is printed only once within 30 seconds.	
Configuration Examples	The following example sets the usage warning threshold globally. <pre>FS#config FS(config)# mmu usage-warn-limit set 90</pre> The following example sets the usage warning threshold for unicast queue 3 and 8 to 80%. <pre>FS#config FS(config)# int te1/1 FS(config-if)# mmu usage-warn-limit unicast 3 8 set 80</pre>	
Platform Description	N/A	

3.5 mmu queue-guarantee

	Use this command to configure the guaranteed buffer. mmu queue-guarantee output { unicast } {<i>queue-id1</i> [<i>queue-id2</i> [<i>queue-idN</i>]] { set <i>value</i>

	Use the no form of this command to restore the default setting. no mmu queue-guarantee output { unicast }	
Parameter Description	Parameter	Description
	output	Performs buffer management on the output queue.
	unicast	Performs buffer management on the output unicast queue.
	<i>queue-idN</i>	Queue ID
	<i>value</i>	Sets the number of guaranteed buffer, in the unit of cells.
Defaults	The default varies with different products.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	This command is executed in different ways on different devices.	
Configuration Examples	The following example configures guaranteed buffer for unicast queue. <pre> FS#config FS(config)# interface tenGigabitEthernet 1/9 FS(config-if)#mmu queue-guarantee ouput unicast 1 3 7 8 set 15 FS(config-if)#exit FS(config)#exit FS# </pre>	
Platform Description	N/A	

3.6 mmu queue-thredshold

	Use this command to configure the shared buffer. mmu queue-thredshold output { unicast } { queue-id1 [queue-id2 [queue-idN]] } set th%	
	Use the no form of this command to restore the default setting. no mmu queue-thredshold output { unicast }	
Parameter Description	Parameter	Description
	output	Performs buffer management on the output queue.
	unicast	Performs buffer management on the output unicast queue.

	<i>queue-idN</i>	Queue ID
	<i>th%</i>	Total shared buffer * threshold = Available buffer
Defaults	The default varies with different products.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example configures shared buffer for unicast queue. <pre>FS#config FS(config)# interface tenGigabitEthernet 1/9 FS(config-if)#mmu queue-threshold ouput unicast 1 3 7 8 set 80 FS(config-if)#exit</pre>	
Platform Description	N/A	

3.7 mmu fc-threshold

	Use this command to configure the inbound buffer threshold. mmu fc-threshold set <i>th%</i>	
	Use the no form of this command to restore the default setting. no mmu fc-threshold	
Parameter Description	Parameter	Description
	<i>th%</i>	Indicates the percentage of inbound buffer threshold.
Defaults	The default varies with different products.	
Command Mode	Interface configuration mode	
Usage Guide	This command is executed in different ways on different devices. This command only takes effect when flow control/PFC is enabled.	
Configuration Examples	The following example configures inbound buffer threshold of priority group. <pre>FS#config FS(config)# interface tenGigabitEthernet 0/9</pre>	

	FS(config-if)#mmu fc-threshold set 80 FS(config-if)#exit
Platform Description	N/A

3.8 show queue-buffer interface

	Use this command to display buffer usage of interfaces. show queue-buffer interface { <i>interface-id</i> }																																																																																																																																																							
Parameter Description	Parameter				Description																																																																																																																																																			
	<i>interface-id</i>				Interface																																																																																																																																																			
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																																																																																																																																																							
Default Level	14																																																																																																																																																							
Usage Guide	N/A																																																																																																																																																							
Configuration Examples	The following example displays buffer usage of the specified interface based on output queue. <pre>FS(config)#show queue-buffer interface hundredGigabitEthernet 0/1</pre> Interface HundredGigabitEthernet 0/1: Slice 1: <table><thead><tr><th>Type</th><th>Queue</th><th>Used cells</th><th>Available cells</th><th>Usage</th><th>Usage warn limit</th><th>Usage warn count</th><th>Peaked cells</th></tr></thead><tbody><tr><td>Unicast</td><td>1</td><td>42288</td><td>0</td><td></td><td>100%</td><td>0%</td><td>0</td></tr><tr><td></td><td></td><td>42288</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>Unicast</td><td>2</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>3</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>4</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>5</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>6</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>7</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Unicast</td><td>8</td><td>0</td><td>42280</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>1</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>3442</td></tr><tr><td>Multicast</td><td>2</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>3</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>4</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>5</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>6</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>7</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr><tr><td>Multicast</td><td>8</td><td>0</td><td>668</td><td>0%</td><td>0%</td><td>0</td><td>0</td></tr></tbody></table>								Type	Queue	Used cells	Available cells	Usage	Usage warn limit	Usage warn count	Peaked cells	Unicast	1	42288	0		100%	0%	0			42288						Unicast	2	0	42280	0%	0%	0	0	Unicast	3	0	42280	0%	0%	0	0	Unicast	4	0	42280	0%	0%	0	0	Unicast	5	0	42280	0%	0%	0	0	Unicast	6	0	42280	0%	0%	0	0	Unicast	7	0	42280	0%	0%	0	0	Unicast	8	0	42280	0%	0%	0	0	Multicast	1	0	668	0%	0%	0	3442	Multicast	2	0	668	0%	0%	0	0	Multicast	3	0	668	0%	0%	0	0	Multicast	4	0	668	0%	0%	0	0	Multicast	5	0	668	0%	0%	0	0	Multicast	6	0	668	0%	0%	0	0	Multicast	7	0	668	0%	0%	0	0	Multicast	8	0	668	0%	0%	0	0
Type	Queue	Used cells	Available cells	Usage	Usage warn limit	Usage warn count	Peaked cells																																																																																																																																																	
Unicast	1	42288	0		100%	0%	0																																																																																																																																																	
		42288																																																																																																																																																						
Unicast	2	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	3	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	4	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	5	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	6	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	7	0	42280	0%	0%	0	0																																																																																																																																																	
Unicast	8	0	42280	0%	0%	0	0																																																																																																																																																	
Multicast	1	0	668	0%	0%	0	3442																																																																																																																																																	
Multicast	2	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	3	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	4	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	5	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	6	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	7	0	668	0%	0%	0	0																																																																																																																																																	
Multicast	8	0	668	0%	0%	0	0																																																																																																																																																	

Slice 3:

Type	Queue	Used cells	Available cells	Usage	Usage warn limit	Usage warn count	Peaked cells
Unicast	1	0	42287	0%	0%	0	0
Unicast	2	0	42287	0%	0%	0	0
Unicast	3	0	42287	0%	0%	0	0
Unicast	4	0	42287	0%	0%	0	0
Unicast	5	0	42287	0%	0%	0	0
Unicast	6	0	42287	0%	0%	0	0
Unicast	7	0	42287	0%	0%	0	0
Unicast	8	0	42287	0%	0%	0	0
Multicast	1	0	5292	0%	0%	0	0
Multicast	2	0	5292	0%	0%	0	0
Multicast	3	0	5292	0%	0%	0	0
Multicast	4	0	5292	0%	0%	0	0
Multicast	5	0	5292	0%	0%	0	0
Multicast	6	0	5292	0%	0%	0	0
Multicast	7	0	5292	0%	0%	0	0
Multicast	8	0	5292	0%	0%	0	0

Slot	Slice	PortGroup	Total cells	Total usage	Usage warn limit	Static used cells	Global shared cells
Available shared cells							
0	1	1	53248	79%	90%	8	47564
5284							
0	2	1	53248	79%	90%	8	47564
5284							
0	3	1	53248	0%	90%	0	47564
47564							
0	4	1	53248	0%	90%	0	47564
47564							

Field	Description
Slice	No. of the module on the chip for buffer division
Type	Queue type, including unicast queue and multicast queue
Queue	Queue No., ranging from 1 to 8 by default and can be switched to 0 to 7 through configuration
Used cells	Size of the occupied buffer in a queue, in the unit of cell
Available cells	Size of the available buffer in a queue, in the unit of cell
Usage	Percentage of the occupied buffer in a queue
Usage warn limit	Buffer usage warning threshold of a specific port group or queue
Usage warn count	Number of times that the occupied buffer exceeds the warning threshold
Peaked cells	Historical peak value of the used buffer
Slot	Slot No. of the line card

	PortGroup	Port group No., starting from 1					
	Total cells	Total buffer on a specified slice					
	Total usage	Percentage of the occupied buffer on a specified slice					
	Static used cells	Size of the occupied guarantee buffer on a specified slice					
	Global shared cells	Total shared buffer on a specified slice					
	Available shared cells	Size of the available shared buffer on a specified slice					

The following example displays the buffer queue information of all interfaces.

```
FS#show queue-buffer
Interface HundredGigabitEthernet 0/1:
Slice 1:
Type      Queue  Used cells  Available cells  Usage  Usage warn limit  Usage warn count  Peaked cells
Unicast   1      22383      1               99%    50%              686
42288
Unicast   2      0          22384           0%     0%              0
Unicast   3      0          22384           0%     0%              0
Unicast   4      22391      0               100%   0%              0
22416
Unicast   5      0          22384           0%     0%              0
Unicast   6      0          22384           0%     0%              0
Unicast   7      0          22384           0%     0%              0
Unicast   8      0          22384           0%     0%              0
Multicast 1      0          357             0%     0%              3442
Multicast 2      0          357             0%     0%              0
Multicast 3      0          357             0%     0%              0
Multicast 4      0          357             0%     0%              0
Multicast 5      0          357             0%     0%              0
Multicast 6      0          357             0%     0%              0
Multicast 7      0          357             0%     0%              0
Multicast 8      0          357             0%     0%              0

Slice 3:
Type      Queue  Used cells  Available cells  Usage  Usage warn limit  Usage warn count  Peaked cells
Unicast   1      0          42287           0%     50%              0
Unicast   2      0          42287           0%     0%              0
Unicast   3      0          42287           0%     0%              0
Unicast   4      0          42287           0%     0%              0
Unicast   5      0          42287           0%     0%              0
Unicast   6      0          42287           0%     0%              0
Unicast   7      0          42287           0%     0%              0
Unicast   8      0          42287           0%     0%              0
Multicast 1      0          5292           0%     0%              0
Multicast 2      0          5292           0%     0%              0
```


Multicast	3	0	5292	0%	0%	0	0
Multicast	4	0	5292	0%	0%	0	0
Multicast	5	0	5292	0%	0%	0	0
Multicast	6	0	5292	0%	0%	0	0
Multicast	7	0	5292	0%	0%	0	0
Multicast	8	0	5292	0%	0%	0	0
Slot Slice PortGroup Total cells Total usage Usage warn limit Static used cells Global shared cells Available shared cells							
0	1	1	53248	84%	90%	16	47564
0	2	1	53248	0%	90%	0	47564
0	3	1	53248	0%	90%	0	47564
0	4	1	53248	0%	90%	0	47564
.....							
Interface HundredGigabitEthernet 0/64:							
Slice 2:							
Type	Queue	Used cells	Available cells	Usage	Usage warn limit	Usage warn count	Peaked cells
Unicast	1	0	42287	0%	0%	0	0
Unicast	2	0	42287	0%	0%	0	0
Unicast	3	0	42287	0%	0%	0	0
Unicast	4	0	42287	0%	0%	0	0
Unicast	5	0	42287	0%	0%	0	0
Unicast	6	0	42287	0%	0%	0	0
Unicast	7	0	42287	0%	0%	0	0
Unicast	8	0	42287	0%	0%	0	0
Multicast	1	0	5292	0%	0%	0	3442
Multicast	2	0	5292	0%	0%	0	0
Multicast	3	0	5292	0%	0%	0	0
Multicast	4	0	5292	0%	0%	0	0
Multicast	5	0	5292	0%	0%	0	0
Multicast	6	0	5292	0%	0%	0	0
Multicast	7	0	5292	0%	0%	0	0
Multicast	8	0	5292	0%	0%	0	0
Slice 4:							
Type	Queue	Used cells	Available cells	Usage	Usage warn limit	Usage warn count	Peaked cells
Unicast	1	0	42287	0%	0%	0	0
Unicast	2	0	42287	0%	0%	0	0
Unicast	3	0	42287	0%	0%	0	0

	Unicast	4	0	42287	0%	0%	0	0
	Unicast	5	0	42287	0%	0%	0	0
	Unicast	6	0	42287	0%	0%	0	0
	Unicast	7	0	42287	0%	0%	0	0
	Unicast	8	0	42287	0%	0%	0	0
	Multicast	1	0	5292	0%	0%	0	0
	Multicast	2	0	5292	0%	0%	0	0
	Multicast	3	0	5292	0%	0%	0	0
	Multicast	4	0	5292	0%	0%	0	0
	Multicast	5	0	5292	0%	0%	0	0
	Multicast	6	0	5292	0%	0%	0	0
	Multicast	7	0	5292	0%	0%	0	0
	Multicast	8	0	5292	0%	0%	0	0
	Slot	Slice	PortGroup	Total cells	Total usage	Usage warn limit	Static used cells	Global shared cells
	Available shared cells							
	0	1	1	53248	84%	90%	16	47564
	2797							
	0	2	1	53248	0%	90%	0	47564
	47564							
	0	3	1	53248	0%	90%	0	47564
	47564							
	0	4	1	53248	0%	90%	0	47564
	47564							
Platform Description	N/A							

3.9 show queue-counter interface

	Use this command to display buffer queue statistics of interfaces. show queue-counter interface <i>interface-id</i>	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Default Level	14	
Usage Guide	N/A	

Configuration

The following example displays buffer queue statistics of the specified interface based on output queue.

Examples

```
FS#show queue-counter interface gigabitEthernet 0/9
```

```
Interface HundredGigabitEthernet 4/1:
```

```
Unicast
```

Queue	Transmitted Bytes	Dropped Bytes	Frame Loss Rate(%)	Transmit Rate(bps)
1		0	0	0
2		0	0	0
3		0	0	0
4		0	0	0
5		0	0	0
6		0	0	0
7		0	0	0
8	62797		0	0

```
656
Multicast
```

Queue	Transmitted Bytes	Dropped Bytes	Frame Loss Rate(%)	Transmit Rate(bps)
1		0	0	0
2		0	0	0
3		0	0	0
4		0	0	0
5		0	0	0
6		0	0	0
7		0	0	0
8		0	0	0

```
Unicast
```

Queue	Transmitted Packets	Dropped Packets	Frame Loss Rate(%)	Transmit Rate(pps)
1		0	0	0
2		0	0	0

0					
0	3		0		0
0	4		0		0
0	5		0		0
0	6		0		0
0	7		0		0
0	8	472		0	0
0	Multicast				
	Queue	Transmitted Packets	Dropped Packets	Frame Loss Rate(%)	Transmit Rate(pps)
0	1		0	0	0
0	2		0	0	0
0	3		0	0	0
0	4		0	0	0
0	5		0	0	0
0	6		0	0	0
0	7		0	0	0
0	8		0	0	0

The following example displays buffer queue statistics of all interfaces.

FS#show queue-counter

Interface HundredGigabitEthernet 0/1:

Unicast

Queue	Transmitted Bytes	Dropped Bytes	Frame Loss Rate(%)	Transmit Rate(bps)
1	117380835776	1056130216960		89.99
50525032				
2		0	0	0
0				
3		0	0	0
0				
4	2736178496	24624019520		89.99

50525056					
5		0	0	0	
0					
6		0	0	0	
0					
7		0	0	0	
0					
8		1200887	0	0	
664					
Multicast					
Queue	Transmitted Bytes	Dropped Bytes	Frame Loss Rate(%)	Transmit Rate(bps)	
1	24098176		233925440	90.66	
0					
2	0	0	0	0	
0					
3	0	0	0	0	
0					
4	0	0	0	0	
0					
5	0	0	0	0	
0					
6	0	0	0	0	
0					
7	0	0	0	0	
0					
8	0	0	0	0	
0					
Unicast					
Queue	Transmitted Packets	Dropped Packets	Frame Loss Rate(%)	Transmit Rate(pps)	
1	1834075559		16502034640	89.99	
75183					
2	0	0	0	0	
0					
3	0	0	0	0	
0					
4	42752789		384750305	89.99	
75183					
5	0	0	0	0	
0					
6	0	0	0	0	
0					
7	0	0	0	0	
0					
8	9306		0	0	

```

0
Multicast
Queue    Transmitted Packets    Dropped Packets    Frame Loss Rate(%)    Transmit Rate(pps)
1          376534                0                  3655085                90.66
0
2          0                    0                  0                      0
0
3          0                    0                  0                      0
0
4          0                    0                  0                      0
0
5          0                    0                  0                      0
0
6          0                    0                  0                      0
0
7          0                    0                  0                      0
0
8          0                    0                  0                      0
0Gi0/24    0                    0                  0                      0.000
.....
Interface HundredGigabitEthernet 0/64:
Unicast
Queue    Transmitted Bytes    Dropped Bytes    Frame Loss Rate(%)    Transmit Rate(bps)
1      83892643136        0                754894738496        89.99
0
2          0                    0                  0                      0
0
3          0                    0                  0                      0
0
4          0                    0                  0                      0
0
5          0                    0                  0                      0
0
6          0                    0                  0                      0
0
7          0                    0                  0                      0
0
8      1203321          0                0                      0
664
Multicast
Queue    Transmitted Bytes    Dropped Bytes    Frame Loss Rate(%)    Transmit Rate(bps)
1      126178880          0                1208592000          90.54
0
2          0                    0                  0                      0

```

0					
0	3		0	0	0
0	4		0	0	0
0	5		0	0	0
0	6		0	0	0
0	7		0	0	0
0	8		0	0	0
0	Unicast				
	Queue	Transmitted Packets	Dropped Packets	Frame Loss Rate(%)	Transmit Rate(pps)
	1	1310822549		11795230289	89.99
0	2		0	0	0
0	3		0	0	0
0	4		0	0	0
0	5		0	0	0
0	6		0	0	0
0	7		0	0	0
	8	9317		0	0
0	Multicast				
	Queue	Transmitted Packets	Dropped Packets	Frame Loss Rate(%)	Transmit Rate(pps)
	1	1971545		18884250	90.54
0	2		0	0	0
0	3		0	0	0
0	4		0	0	0
0	5		0	0	0
0	6		0	0	0

	0	7	0	0	0
	0	8	0	0	0
	0				
Platform Description	N/A				

IP Routing Commands

1 RIP Commands

1.1 address-family

	Use this command to configure the RIP protocol in address family configuration sub-mode. Use the no form of this command to restore the default setting.	
	address-family ipv4 vrf <i>vrf-name</i>	
	no address-family ipv4 vrf <i>vrf-name</i>	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	Specifies the VRF name associated with the sub-mode command.
Defaults	The address family of the RIP protocol is not configured by default.	
Command Mode	Route configuration mode	
Usage Guide	Use the address-family command to enter the address family configuration sub-mode. The prompt is (config-router-af) #. When you specify the VRF associated with the sub-mode for the first time, the RIP instance corresponding to the VRF will be created. In the sub-mode, you can configure the VRF RIP routing information. To remove the address family sub-mode and return to the route configuration mode, use the exit-address-family or exit command.	
Configuration Examples	The following example creates a VRF with the name of vpn1 and creates its RIP instance. <pre> FS(config)# ip vrf vpn1 FS(config-vrf)# exit FS(config)# interface fastEthernet 1/0 FS(config-if-FastEthernet 0/1)# ip vrf forwarding vpn1 FS(config-if-FastEthernet 0/1)# ip address 192.168.1.1 255.255.255.0 FS(config)# router rip FS(config-router)# address-family ipv4 vrf vpn1 FS(config-router)# network 192.168.1.0 FS(config-router)# exit-address-family </pre>	
Related Commands	Command	Description
	exit-address-family	Exits the address family configuration sub-mode.
	ip vrf	Creates a VRF.
Platform	N/A	

Description	

1.2 auto-summary

	Use this command to enable automatic summary of RIP routes. Use the no form of this command to disable this function	
	auto-summary	
	no auto-summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Automatic summary of RIP routes is enabled by default	
Command Mode	Routing progress configuration mode	
Usage Guide	Automatic RIP route summary means the subnet routes will be automatically summarized into the routes of the classified network when they traverse through the subnet. Automatic route summary is enabled by default for RIPv1 and RIPv2. Automatic RIP route summary improves the flexibility and effectiveness of the network. If the summarized route exists, the sub-routes contained in the summarized route cannot be seen in the routing table, reducing the size of the routing table significantly. Advertising the summarized route is more efficient than advertising individual routes in light of the following factors: ● The summarized route is always processed preferentially when you query the RIP database. ● Any sub-route is ignored when you query the RIP database, reducing the processing time. ● If you want to learn the specific sub-routes instead of the summarized route, disable the automatic route summary function. Only when RIPv2 is configured, the automatic route summary function can be disabled. For the RIPv1, the automatic route summary function is always enabled.  The range of the supernet route is wider than that of the classful network. Therefore, this command takes no effect on the supernet route.	
Configuration Examples	The following example disables automatic route summary of RIPv2. <pre>FS (config)# router rip FS (config-router)# version 2 FS (config-router)# no auto-summary</pre>	
Related Commands	Command	Description
	version	Defines the RIP software versions: v1 or v2. Both v1

		and v2 are supported by default.
Platform Description	N/A	

1.3 bfd all-interfaces

	Use this command to enable all interfaces running RIP to use the BFD function. Use the no form of this command to restore the default setting.	
	bfd all-interfaces	
	no bfd all-interfaces	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	BFD is not configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	With the BFD function enabled on the RIP, one BFD session will be established for the RIP routing information source (the source address of the RIP route update packet). Once the BFD neighbor fails, the RIP routing information will be invalid directly and no longer join routing or forwarding. You can also use the interface configuration mode command ip rip bfd [disable] to enable or disable the BFD function on the specified interface, which takes precedence over the command bfd all-interfaces in the routing progress configuration mode.	
Configuration Examples	N/A	
Related Commands	Command	Description
	route ip	Creates the RIP routing progress and enters the routing process configuration mode.
	ip rip bfd [disable]	Configures a specified interface running RIP to enable or disable link detection using the BFD.
Platform Description	N/A	

1.4 default-information originate

	Use this command to generate a default route in the RIP progress. Use the no form of this command to delete the generated default route.

	default-information originate [always] [metric <i>metric-value</i>] [route-map <i>map-name</i>]	
	no default-information originate [always] [metric] [route-map <i>map-name</i>]	
Parameter Description	Parameter	Description
	always	(Optional) Enables RIP to generate the default route, no matter whether the default route exists or not.
	metric <i>metric-value</i>	(Optional) The original metric value of the default route with the value range 1 to 15 of <i>metric-value</i> .
	route-map <i>map-name</i>	(Optional) Name of the associated route-map. Route-map is not associated by default.
Defaults	No default route is generated by default. The default metric value is 1.	
Command Mode	Routing process configuration mode	
Usage Guide	By default, RIP will not advertise the default route if the default route exists in the routing table of the router. In this case, use the default-information originate command to notify the neighbor of the default route. With the parameter always configured, no matter whether the default route exists in the RIP routing process or not, the default route will be advertised to the neighbor but is not shown in the local routing table. You can use the show ip rip database command to view the RIP routing information database to confirm whether the default route is generated. Use the parameter route-map to control more about the default route advertised to RIP. For example, use the set metric command to set the metric value of the default route. The route-map set metric rule takes precedence over the parameter metric value configuration of the default route. If the parameter metric is not configured, the default metric value is used by the default route.  If the default route can be generated in the RIP process by using this command, RIP will not learn the default route advertised from the neighbor.  For the default route generated by using the ip default-network command, the default-information originate command is required to add the default route to RIP.	
Configuration Examples	The following example generates a default route to the RIP routing table. <pre>FS(config-router)# default-information originate always</pre>	
Related Commands	Command	Description
	ip rip default-information	Notifies the default route through an interface.
	redistribute	Redistributes the routes from other protocols to RIP.
Platform Description	N/A	

1.5 default-metric

	Use this command to define the default RIP metric value. Use the no form of this command to restore the default setting.	
	default-metric <i>metric-value</i>	
	no default-metric	
Parameter Description	Parameter	Description
	<i>metric-value</i>	Indicates the default metric value with the range from 1 to 16. If the metric value is greater than or equal to 16, the RGNOS regards the route unreachable.
Defaults	The default is 1.	
Command Mode	Routing process configuration mode	
Usage Guide	This command needs to work with the command redistribute . When the routes are redistributed to the RIP routing process from a routing protocol process, the route metric value cannot be converted due to the incompatibility of the metric calculation mechanisms for different protocols. During the conversion, therefore, it is required to redefine the metric values of redistributed routes in the RIP routing domain. If there is no clear definition of the metric value in redistributing a routing protocol process, the RIP uses the metric value defined with default-metric . If the metric value is defined, this value overwrites the metric value defined with default-metric. If this command is not configured, the default value of default-metric is 1.	
Configuration Examples	The following example enables the RIP routing protocol to redistribute the routes learned by the OSPF routing protocol, whose initial RIP metric value is set to 3. <pre> FS (config)# router rip FS (config-router)# default-metric 3 FS (config-router)# redistribute ospf 100 </pre>	
Related Commands	Command	Description
	redistribute	Redistributes the routes from one routing domain to another routing domain.
Platform Description	N/A	

1.6 distance

	Use this command to set the management distance of the RIP route. Use the no form of this command to restore the default setting.

	distance <i>distance</i> [<i>ip-address wildcard</i>]	
	no distance [<i>distance ip-address wildcard</i>]	
Parameter Description	Parameter	Description
	<i>distance</i>	Sets the management distance of a RIP route, an integer in the range from 1 to 255.
	<i>ip-address</i>	Indicates the prefix of the source IP address of the route.
	<i>wildcard</i>	Defines the comparison bit of the IP address, where 0 means accurate matching and 1 means no comparison.
Defaults	The default is 120.	
Command Mode	Routing process configuration mode	
Usage Guide	Use this command to set the management distance of the RIP route. You can use this command to create several management distances with source address prefixes. When the source address of the RIP route is within the range specified by the prefixes, the corresponding management distance is applied; otherwise, the route uses the management distance configured by the RIP.	
Configuration Examples	The following example sets the management distance of the RIP route to 160, and specifies the management distance of the route learned from 192.168.2.1 as 123. <pre>FS(config)# router rip FS(config-router)# distance 160 FS(config-router)# distance 123 192.168.12.1 0.0.0.0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.7 distribute-list in

	Use this command to control route update for route filtering. Use the no form of this command to restore the default setting.
	distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>] [gateway <i>prefix-list-name</i>] } in [<i>interface-type interface-number</i>]
	no distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>] [gateway <i>prefix-list-name</i>] } in [<i>interface-type interface-number</i>]

Parameter Description	Parameter	Description
	<i>access-list-number</i> <i>name</i>	Specifies the ACL. Only the routes that are allowed by the ACL can be accepted.
	prefix <i>prefix-list-name</i>	Uses the prefix list to filter the routes.
	gateway <i>prefix-list-name</i>	Uses the prefix list to filter the source of the routes.
	<i>interface-type</i> <i>interface-number</i>	(Optional) Applies the distribution list only to a specified interface.
Defaults	The distribution list is not defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	To deny receiving some specified routes, you can process all the received route update packets by configuring the route distribute control list. Without any interface specified, the system will process the route update packets received on all the interfaces.	
Configuration Examples	The following example enables RIP to control the routes received from the Fastethernet 0/0, only permitting the routes starting with 172.16. <pre> FS (config)# router rip FS (config-router)# network 200.168.23.0 FS (config-router)# distribute-list 10 in fastethernet 0/0 FS (config-router)# no auto-summary FS (config-router)# access-list 10 permit 172.16.0.0 0.0.255.255 </pre>	
Related Commands	Command	Description
	access-list	Defines the ACL rule.
	prefix-list	Defines the prefix list.
Platform Description	N/A	

1.8 distribute-list out

	Use this command to control route update advertisement for filtering routes. Use the no form of this command to restore the default setting.
	distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> } out [<i>interface</i> [bgp connected isis] [<i>area-tag</i>] ospf <i>process-id</i> rip static]]
	no distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> } out [<i>interface</i> [bgp connected isis] [<i>area-tag</i>] ospf <i>process-id</i> rip static]]

Parameter Description	Parameter	Description
	<i>access-list-number name</i>	Specifies the ACL.
	<i>prefix prefix-list-name</i>	Uses the prefix list to filter routes.
	<i>interface</i>	(Optional) Applies route update advertisement control to a specified interface in the distribution list.
	<i>bgp</i>	(Optional) Applies route update advertisement control to only routes introduced from bgp in this distribution list.
	<i>connected</i>	(Optional) Applies route update advertisement control to only connected routes in this distribution list.
	<i>isis [area-tag]</i>	(Optional) Applies route update advertisement control to only routes introduced from ISIS in this distribution list. <i>area-tag</i> specifies an ISIS instance.
	<i>ospf process-id</i>	(Optional) Applies route update advertisement control to only routes introduced from OSPF in this distribution list. <i>process-id</i> specifies an OSPF instance.
	<i>rip</i>	(Optional) Applies route update advertisement control to only RIP routes in this distribution list.
	<i>static</i>	(Optional) Applies route update advertisement control to only static routes in this distribution list.
Defaults	No route update advertisement is configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	If this command relates to none of optional parameters, route update advertisement control applies to all interfaces. If this command relates to interface options, route update advertisement control applies to only the specified interface. If this command relates to other route process parameters, route update advertisement control applies to only the specific route process.	
Configuration Examples	The following example advertises only the 192.168.12.0/24 route. <pre> FS (config)# router rip FS (config-router)# network 200.4.4.0 FS (config-router)# network 192.168.12.0 FS (config-router)# distribute-list 10 out FS (config-router)# version 2 FS (config-router)#access-list 10 permit 192.168.12.0 0.0.0.255 </pre>	
Related Commands	Command	Description
	<i>access-list</i>	Defines the ACL rule.
	<i>prefix-list</i>	Defines the prefix list.
	<i>redistribute</i>	Configures route redistribution.
Platform Description	N/A	

1.9 enable mib-binding

	Use this command to bind a MIB with a specified RIP instance. Use the no form of this command to restore the default setting	
	enable mib-binding	
	no enable mib-binding	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the MIB is bound with the RIP instance of the default VRF.	
Command Mode	Routing process configuration mode.	
Usage Guide	As RIP MIB does not have RIP instance information, you can only operate only one RIP instance using SNMP. By default, RIP MIB is bound with the RIP instance of the default VRF. You can only operate this RIP instance. If you want to operate another RIP instance of a specified VRF through SNMP, you can use this command to bind the MIB with this instance.	
Configuration Examples	The following example operates the RIP instance of a specified VRF, vpn1. <pre>FS(config)# router rip FS(config-router)# address-family ipv4 vrf vpn1 FS(config-router-af)# enable mib-binding</pre>	
Related Commands	Command	Description
	show ip rip	Displays the global configuration of RIP.
Platform Description	N/A	

1.10 exit-address-family

	Use this command to exit the address family configuration mode	
	exit-address-family	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	

Command		
Mode	Address family configuration mode	
Usage Guide	Use this command to exit the address family configuration mode. The abbreviation of this command is exit.	
Configuration Examples	The following example enters or exits the address family configuration mode. FS(config-router)# address-family ipv4 vrf vpn1 FS(config-router-af)# exit-address-family	
Related Commands	Command	Description
	address-family	Enters the address family configuration sub-mode.
Platform Description	N/A	

1.11 fast-reroute

	Use this command to enable the RIP FRR (Fast Reroute) function for the device. Use the no form of this command to restore the default setting.	
	fast-reroute route-map <i>route-map-name</i>	
	no fast-reroute	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	Specifies the backup path through the route map.
Defaults	This function is disabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	Use the route-map command to specify the backup path for the matched routes. It is recommended to enable the BFD function when the RIP fast reroute function is enabled. BFD allows the device to detect the link fault faster, so as to reduce the interruption time. In the scenario where the port is up/down, it is recommended to configure carrier-delay 0 in interface configuration mode to achieve the fastest switchover speed, reducing the interruption time. Currently, the restrictions of the RIP FRR are as follows: Only one backup next hop is generated for each route. The backup next hop is not generated for the ECMP route.	
Configuration Examples	The following example enables FRR for RIP instance 1 and associates route map <i>fast reroute</i> .	
	FS(config)# route-map fast-reroute	

	<pre>match interface gigabitEthernet 0/2 set fast-reroute backup-interface GigabitEthernet 0/1 backup-nexthop 192.168.1.1 FS(config)# router rip FS(config-router)# fast-reroute route-map fast-reroute</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.12 graceful-restart

	Use this command to configure the RIP graceful restart (GR) function for a device. Use the no form of this command to restore the default configuration.	
	graceful-restart [grace-period <i>grace-period</i>]	
	no graceful-restart [grace-period]	
Parameter Description	Parameter	Description
	graceful-restart	Enables the GR function.
	grace-period	(Optional) Configures the grace period.
	<i>grace-period</i>	(Optional) Indicates the user-defined GR period. The default value is the smaller value between twice the update time and 60 seconds. The range is from 1 to 1,800. The unit is second.
Defaults	This function is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The GR function is configured on the RIP instances. Different parameters can be configured for different RIP instances. The GR period refers to the time from the startup to the end of RIP GR. During this period, the forwarding table remains unchanged and the RIP route is restored to the state before protocol restart. When the GR period expires, RIP exits the GR state and performs normal RIP operation. The graceful-restart grace-period command enables users to modify GR period. Note: Make sure that GR is completed before the RIP route is validate and after an RIP route update cycle elapses. If an improper value is configured, non-stop data forwarding cannot be ensured during the GR process. For example, if the GR period is longer than the time when the neighbor's route is unavailable and GR is not completed before the route is validated, then the neighbor is not re-informed of the route and forwarding of the neighbor's route is terminated when it is validated, which results in data forwarding interruption. Therefore, unless otherwise specified, it is	

	not recommended to adjust the GR period. If the period needs to be changed, determine that the grace period is longer than the route update cycle and shorter than the time when the route is unavailable in combination with the configuration of the timers basic command.	
	 During the RIP GR period, the network must be stable.	
Configuration Examples	The following example enables the RIP GR function and configures the GR period parameters of the GR function. FS(config)# router rip FS(config-router)# graceful-restart grace-period 90	
Related Commands	Command	Description
	timers basic	Configures RIP timers.
Platform Description	N/A	

1.13 ip rip authentication key-chain

	Use this command to enable RIP authentication and specify the keychain used for RIP authentication. Use the no form of this command to restore the default setting.	
	ip rip authentication key-chain <i>name-of-keychain</i>	
	no ip rip authentication key-chain	
Parameter Description	Parameter	Description
	<i>name-of-keychain</i>	Indicates the name of the keychain, which specifies the keychain used for RIP authentication.
Defaults	The keychain is not associated by default.	
Command Mode	Interface configuration mode	
Usage Guide	If the keychain is specified in the interface configuration, use the key chain global configuration command to define the keychain. Otherwise, RIP data packet authentication fails. RIPv2 instead of RIPv1 supports authentication of the RIP data packet.	
Configuration Examples	The following example enables RIP authentication on the fastEthernet 0/1 with the associated keychain ripchain. FS (config)#interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)#ip rip authentication key-chain ripchain Meanwhile, use the key chain command to define this keychain in global configuration mode. FS(config)#key chain <i>ripchain</i>	

	FS(config-keychain)#key 1 FS(config-keychain-key)#key-string Hello	
Related Commands	Command	Description
	ip rip authentication mode	Defines the RIP authentication mode.
	ip rip authentication text-password	Enables RIP authentication, and sets the password string of RIP plaintext authentication. RIP data packet authentication is supported only by RIPv2.
	ip rip receive version	Defines the version of RIP packets received on the interface.
	ip rip send version	Defines the version of RIP packets sent on the interface.
	key chain	Defines the keychain and enters keychain configuration mode.
Platform Description	N/A	

1.14 ip rip authentication mode

	Use this command to define the RIP authentication mode. Use the no form of this command to restore the default setting.	
	ip rip authentication mode { text md5 }	
	no ip rip authentication mode	
Parameter Description	Parameter	Description
	text	Configures RIP authentication as plaintext authentication.
	md5	Configures RIP authentication as MD5 authentication.
Defaults	It is plaintext authentication by default.	
Command Mode	Interface configuration mode	
Usage Guide	During the RIP authentication configuration process, the RIP authentication modes of all devices requiring exchange of RIP routing information must be the same. Otherwise, RIP packet exchange will fail. If the plaintext authentication mode is adopted, but the password string of the plaintext authentication or the associated keychain is not configured, no authentication occurs. In the same way, if the MD5 authentication mode is adopted, but the associated keychain is not configured, no authentication occurs. RIPv2 instead of RIPv1 supports authentication of the RIP data packet.	
Configuration	The following example configures the RIP authentication mode on the fastEthernet 0/1 as MD5.	

Examples	FS (config)#interface fastEthernet 0/1	
	FS (config-if-FastEthernet 0/1)# ip rip authentication mode md5	
Related Commands	Command	Description
	ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication of the RIP data packet.
	ip rip authentication text-password	Enables the RIP authentication mode, and sets the password string of RIP plaintext authentication. Only RIPv2 supports authentication of the RIP data packet.
	key chain	Defines the keychain and enters the keychain configuration mode
Platform Description	N/A	

1.15 ip rip authentication text-password

	Use this command to enable RIP authentication and set the password string of RIP plaintext authentication. Use the no form of this command to restore the default setting.	
	ip rip authentication text-password [0 7] password-string	
	no ip rip authentication text-password	
Parameter Description	Parameter	Description
	0	Specifies that the key is displayed as plaintext.
	7	Specifies that the key is displayed as cipher text.
	<i>password-string</i>	Indicates the password string of the plaintext authentication, in the length of 1-16 bytes.
Defaults	No password string of RIP plaintext authentication is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command works only in plaintext authentication mode. To enable the RIP plaintext authentication function, use this command to configure the corresponding password string, or use the associated key chain to obtain the password string. The latter takes the precedence over the former one. RIPv1 does not support RIP authentication but RIPv2 does.	
Configuration Examples	The following example enables the RIP plaintext authentication on fastEthernet 0/1 and sets the password string to hello.	

	<pre>FS(config)#interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip rip authentication text-password hello</pre>	
Related Commands	Command	Description
	ip rip authentication mode	Defines the RIP authentication mode.
	ip rip authentication key-chain	Enables the RIP authentication mode and specifies the keychain used for RIP authentication. Only RIPv2 supports authentication.
Platform Description	N/A	

1.16 ip rip bfd

	Use the ip rip bfd [disable] command to configure the specified interface running RIP to enable or disable link detection using the BFD. Use the no form of this command to restore the default setting.	
	ip rip bfd [disable]	
	no ip rip bfd	
Parameter Description	Parameter	Description
	disable	Disables the specified interface running RIP and uses the BFD mechanism to perform link detection.
Defaults	Interfaces running RIP are not configured by default. The BFD configuration in RIP process configuration mode is a reference.	
Command Mode	Interface configuration mode	
Usage Guide	The priority of the interface is higher than that of the bfd all-interfaces command in process configuration mode. You can use the ip rip bfd command to enable the BFD to perform link detection on the specified interface according to the actual environment or use the bfd all-interfaces command to configure all interfaces running RIP and enable the BFD to perform link detection. In addition, you can use the ip rip bfd disable command to disable the BFD detection function on the specified interface.	
Configuration Examples	N/A	
Related Commands	Command	Description
	route ip	Enables the RIP routing process and enters the routing process configuration mode.

	bdf all-interfaces	Configures all interfaces running RIP to use the BFD to perform link detection.
Platform Description	N/A	

1.17 ip rip default-information

	Use this command to advertise the default route through a RIP interface. Use the no form of this command to restore the default setting.	
	ip rip default-information { only originate } [metric <i>metric-value</i>]	
	no ip rip default-information	
Parameter Description	Parameter	Description
	only	Notifies the default route rather than other routes.
	originate	Notifies the default route and other routes.
	metric <i>metric-value</i>	Specifies the metric value of the default route, in the range from 1 to 15.
Defaults	No default route is configured by default. The default metric value is 1.	
Command Mode	Interface configuration mode	
Usage Guide	After you configure this command on a specified interface, a default route is generated and notified through the interface. If the ip rip default-information command of the interface and the default-information originate command of the RIP process are configured at the same time, only the default route of the interface is advertised.  RIP will no longer learn the default route notified by the neighbor if any interface is configured with the ip rip default-information command.	
Configuration Examples	The following example creates a default route which is notified on ethernet0/1 only. <pre>FS(config)#interface ethernet 0/1 FS(config-if-Ethernet 0/1)#ip rip default-information only</pre>	
Related Commands	Command	Description
	default-information originate	Generates a default route in the RIP process.
Platform Description	N/A	

1.18 ip rip receive enable

	Use this command to enable RIP to receive the RIP data package on a specified interface. Use the no form of this command to restore the default setting.	
	ip rip receive enable	
	no ip rip receive enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	RIP packages can be received through the interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	To prevent an interface from receiving RIP packets, use the no form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the default form of this command to enable the interface to receive the RIP data package.	
Configuration Examples	The following example prohibits receiving RIP data packages on fastEthernet 0/1. <pre>FS (config)# interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)# no ip rip receive enable</pre>	
Related Commands	Command	Description
	ip rip send enable	Enables or disables the interface to send RIP data packages.
	passive-interface	Configures a passive RIP interface.
Platform Description	N/A	

1.19 ip rip receive version

	Use this command to define the version of RIP packets received on an interface. Use the no form of this command to restore the default setting.	
	ip rip receive version [1] [2]	
	no ip rip receive version	
Parameter Description	Parameter	Description
	1	(Optional) Receives only RIPv1 packets.
	2	(Optional) Receives only RIPv2 packets.

Defaults	The default behavior depends on the configuration with the version command.				
Command Mode	Interface configuration mode				
Usage Guide	This command overwrites the default configuration of the version command. It affects only RIP packet receiving through the interface and allows RIPv1 and RIPv2 packets to be received on the interface at the same time. If the command is configured without parameters, data package receiving depends on the configuration of the version.				
Configuration Examples	The following example enables receiving both RIPv1 and RIPv2 data packages. <pre>FS (config)#interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)# ip rip receive version 1 2</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>version</td><td>Defines the default version of the RIP packets received/sent on the interface.</td></tr> </table>	Command	Description	version	Defines the default version of the RIP packets received/sent on the interface.
Command	Description				
version	Defines the default version of the RIP packets received/sent on the interface.				
Platform Description	N/A				

1.20 ip rip send enable

	Use this command to enable RIP to send a RIP data package on a specified interface. Use the no form of this command to restore the default setting.	
	ip rip send enable	
	no ip rip send enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	RIP packages can be sent through the interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	To prevent an interface from sending RIP packets, use the no form of this command in interface configuration mode. This command works on interfaces configured with this command. You can use the default form of this command to enable the interface to send the RIP data package.	
Configuration Examples	The following example prohibits sending RIP data packages on fastEthernet 0/1. <pre>FS (config)# interface fastEthernet 0/1</pre>	

	FS (config-if-FastEthernet 0/1)# no ip rip send enable	
Related Commands	Command	Description
	ip rip receive enable	Enables or disables receiving RIP packets on the interface.
	passive-interface	Configures a passive RIP interface.
Platform Description	N/A	

1.21 ip rip send supernet-routes

	Use this command to enable RIP to send the supernet route on a specified interface. Use the no form of this command to disable this function.	
	ip rip send supernet-routes	
	no ip rip send supernet-routes	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	When the RIPv1 router monitors a RIPv2 router response packet and if the supernet routing information is monitored, incorrect route information is learned because the RIPv1 ignores the subnet mask of the routing information. In this case, you are advised to use the no form of this command on the RIPv2 router to disable advertising the supernet route on the corresponding interface. This command works only on interfaces configured with this command.  This command is only valid upon sending the RIPv2 packets on the interface and it is used to control sending the supernet route.	
Configuration Examples	The following example disables sending RIP supernet routes on the fastEthernet 0/1 interface. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# no ip rip send supernet-routes</pre>	
Related Commands	Command	Description
	version	Defines the RIP version
	ip rip send enable	Enables or disables sending the RIP package on the

	interface.
Platform Description	N/A

1.22 ip rip send version

	Use this command to define the version of the RIP packets sent on the interface. Use the no form of this command to restore the default setting.	
	ip rip send version [1] [2]	
	no ip rip send version	
Parameter Description	Parameter	Description
	1	(Optional) Receives only RIPv1 packets.
	2	(Optional) Receives only RIPv2 packets.
Defaults	The default behavior depends on the configuration with the version command.	
Command Mode	Interface configuration mode	
Usage Guide	This command overwrites the default configuration of the version command. It affects only RIP packet sending through the interface and allows RIPv1 and RIPv2 packages sent on the interface at the same time. If the command is configured without parameters, package receiving depends on the configuration of the version.	
Configuration Examples	The following example enables sending both RIPv1 and RIPv2 packages on the fastEthernet 0/1 interface. FS (config)# interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)# ip rip send version 1 2	
Related Commands	Command	Description
	version	Defines the default version of the RIP packets received/sent on the interfaces.
Platform Description	N/A	

1.23 ip rip split-horizon

	Use this command to enable split horizon. Use the no form of this command to disable this function.
	ip rip split-horizon [poisoned-reverse]
	no ip rip split-horizon [poisoned-reverse]

Parameter Description	Parameter	Description
	poisoned-reverse	(Optional) Enables split horizon with poisoned reverse.
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	When multiple devices are connected to the IP broadcast network and run a distance vector routing protocol, the split horizon mechanism is required to prevent loop. The split horizon prevents the device from advertising routing information from the interface that learns that information, which optimizes routing information exchange between multiple devices. For non-broadcast multi-path access networks (such as frame relay and X.25), split horizon may cause some devices to be unable to learn all routing information. Split horizon may need to be disabled in this case. If an interface is configured the secondary IP address, attentions shall be paid also for split horizon. If the poisoned-reverse parameter is configured, split horizon with poisoned reverse is enabled. In this case, devices still advertise the route information through the interface from which the route information is learned. However, the metric value of the route information is set to unreachable. The RIP routing protocol is a distance vector routing protocol, and the split horizon issue shall be cautioned in practical applications. If it is unsure whether split horizon is enabled on the interface, use the show ip rip command to judge. This function makes no influence on the neighbor defined with the neighbor command.	
Configuration Examples	The following example disables the RIP split horizon function on the interface fastethernet 0/0. <pre>FS (config)# interface fastethernet 0/1 FS (config-if)# no ip rip split-horizon</pre>	
Related Commands	Command	Description
	neighbor (RIP)	Defines the IP address of the neighbor of RIP.
	validate-update-source	Enables the source address authentication of the RIP route update message.
Platform Description	N/A	

1.24 ip rip subvlan

	Use this command to enable RIP on super VLANs. Use the no form of this command to restore the default setting. <pre>ip rip subvlan [all vid] no ip rip subvlan</pre>	
Parameter Description	Parameter	Description
	all	Indicates that packets are allowed to be sent to all sub VLANs.

	<i>vid</i>	Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Defaults	The default setting takes effect only on super VLANs with RIP disabled.	
Command Mode	Interface configuration mode	
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.	
Configuration Examples	The following example sends the RIP multicast packets to sub VLAN 1024 of super VLAN 300. <pre>FS(config)# interface vlan 300 FS(config-if-VLAN 300)# ip rip subvlan 1024</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.25 ip rip summary-address

	Use this command to configure port-level convergence through an interface. Use the no form of this command to disable this function.	
	ip rip summary-address <i>ip-address ip-network-mask</i>	
	no ip rip summary-address <i>ip-address ip-network-mask</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Indicates the IP addresses to be converged.
	<i>ip-network-mask</i>	Indicates the subnet mask of the specified IP address for route convergence.
Defaults	The RIP routes are automatically converged to the classful network edge by default.	

Command Mode	Interface configuration mode	
Usage Guide	The ip rip summary-address command converges an IP address or a subnet on a specified port. RIP routes are automatically converged to the classful network edge. The classful subnet can be configured through only port convergence.  The summary range configured by this command cannot be a super class network, that is, the configured mask length is greater than or equal to the natural mask length of the network.	
Configuration Examples	The following example disables the automatic route convergence function of RIPv2. Interface convergence is configured so that fastEthernet 0/1 advertises the converged route 172.16.0.0/16. <pre> FS (config)# interface fastEthernet 0/1 FS (config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0 FS (config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0 FS (config)# router rip FS (config-router)# network 172.16.0.0 FS (config-router)# version 2 FS (config-router)# no auto-summary </pre>	
Related Commands	Command	Description
	auto-summary	Enables the automatic convergence of RIP routes.
Platform Description	N/A	

1.26 ip rip triggered

	Use this command to enable triggered RIP based on links. Use the no form of this command to restore the default setting.	
	ip rip triggered	
	ip rip triggered retransmit-timer <i>timer</i>	
	ip rip triggered retransmit-count <i>count</i>	
	no ip rip triggered	
	no ip rip triggered retransmit-timer	
	no ip rip triggered retransmit-count	
Parameter Description	Parameter	Description
	retransmit-timer <i>timer</i>	Configures the interval at which the Update Request and Update Response packets are retransmitted. The range is from 1 to 3,600. The unit is second. The default is five.
	retransmit-count <i>count</i>	Configures the maximum times that the Update Request and Update

		Response packets are retransmitted. The range is from 1 to 3600. The default is 36.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Triggered RIP (TRIP) is the extension of RIP on the wide area network (WAN), mainly used for demand-based links. With the TRIP function enabled, RIP no longer sends route updates periodically and sends route updates to the WAN interface only if: - Update Request packets are received. - RIP routing information is changed. - Interface state is changed. - The router is started. As periodical RIP update is disabled, the confirmation and retransmission mechanism is required to ensure that update packets are sent and received successfully over the WAN. The retransmit-timer and retransmit-count commands can be used to specify the retransmission interval and maximum retransmission times for request and update packets.  The function can be enabled in the case of the following conditions: a) The interface has only one neighbor. b) There are multiple neighbors but they interact information using unicast packets. You are advised to enable the function for link layer protocols such as PPP, frame relay, and X.25.  You are advised to enable split horizon with poison reverse on the interface enabled with the function; otherwise invalid routing information might be left.  Make sure that the function is enabled on all routers on the same link; otherwise the function will be invalid and the routing information cannot be exchanged correctly.  The function cannot be enabled at the same time with BFD and RIP functions.  To enable the function, make sure that the RIP configuration is the same on both ends of the link, such as RIP authentication and the RIP version supported by the interface.  If this function is enabled on this interface, the source address of packets on this interface will be checked no matter whether the source IP address verification function (validate-update-source) is enabled.	
Configuration Examples	The following example enables TRIP and sets the retransmission interval and maximum retransmission time to 10 seconds and 18 respectively for Update Request and Update Response packets. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip rip triggered FS(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10 FS(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18</pre>	

Related Commands	Command	Description
	show ip rip database	Displays the summarized routing information of the RIP database.
	show ip rip interface	Displays the RIP interface information.
	ip rip split-horizon	Configures RIP split horizon.
Platform Description	N/A	

1.27 ip rip v2-broadcast

	Use this command to send RIPv2 packets in broadcast rather than multicast mode. Use the no form of this command to restore the default setting.	
	ip rip v2-broadcast	
	no ip rip v2-broadcast	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The default behavior depends on the configuration of the version command.	
Command Mode	Interface configuration mode	
Usage Guide	This command overwrites the default of the version command. This command affects only sending RIP packets on the interface. This command allows RIPv1 and RIPv2 packages sent on the interface simultaneously. If this command is configured without parameters, package receiving depends on the version setting.	
Configuration Examples	The following example sends RIPv2 packets in broadcast mode on the fastEthernet 0/1 interface. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# no ip rip split-horizon</pre>	
Related Commands	Command	Description
	version	Defines the default version of the RIP packets received and sent on the interface.
Platform Description	N/A	

1.28 neighbor

	Use this command to define the IP address of a RIP neighbor. Use the no form of this command to restore the default setting.	
	neighbor <i>ip-address</i>	
	no neighbor <i>ip-address</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Indicates the IP address of the neighbor. The IP address must be that of the network connected to the local device.
Defaults	The neighbor is not defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, and RIPv2 uses the multicast address 224.0.0.9 to do so. If you do not want to allow all the devices on the broadcast network or non-broadcast multi-path access network to receive routing information, use the passive-interface command to configure related interfaces as passive interfaces and then define only some neighbors who can receive the routing information. This command has no impact on the receiving of RIP information. The passive interface is configured. No request packet is sent after the interface is enabled.	
Configuration Examples	The following example creates a VRF with the name of vpn1 and creates its RIP instance. <pre> FS(config)# router rip FS(config-router)# passive-interface default FS(config-router)# neighbor 192.168.1.2 </pre>	
Related Commands	Command	Description
	passive-interface	Configures the interface as a passive interface.
Platform Description	N/A	

1.29 network

	Use this command to define the list of networks to be advertised in the RIP routing process. Use the no form of this command to delete the defined network.	
	network <i>network-number</i> [<i>wildcard</i>]	
	no network <i>network-number</i> [<i>wildcard</i>]	

Parameter Description	Parameter	Description
	<i>network-number</i>	Indicates the network number of the directly-connected network. The network number is a natural one. All interfaces whose IP addresses belong to that natural network can send/receive RIP packages.
	<i>wildcard</i>	Defines the IP address comparing bit: 0 refers to accurate matching, and 1 refers to no comparison.
Defaults	N/A	
Command Mode	Routing process configuration mode	
Usage Guide	The <i>network-number</i> and <i>wildcard</i> parameters can be configured simultaneously to enable the IP address of the interface within the IP address range to join RIP running. Without the <i>wildcard</i> parameter, FSOS make the interface IP address within the classful address range join the RIP running. Only when the IP address of an interface is in the network list defined by RIP, RIP route update packets can be received and sent on the interface.	
Configuration Examples	The following example defines two network numbers associated with RIP and allows the interface IP address between 192.168.12.0/24 and 172.16.0.0/24 to join RIP running. <pre>FS (config)# router rip FS (config-router)# network 192.168.12.0 FS (config-router)# network 172.16.0.0 0.0.0.255</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.30 offset-list

	Use this command to increase the metric value of received or sent RIP routes. Use the no form of this command to restore the default setting.	
	offset-list { access-list-number name } { in out } offset [interface-type interface-number]	
	no offset-list { access-list-number name } { in out } offset [interface-type interface-number]	
Parameter Description	Parameter	Description
	<i>access-list-number</i> <i>name</i>	Specifies the ACL.
	in	Modifies the metric of the received routes using the ACL.

	out	Modifies the metric of the sent routes using the ACL.
	<i>offset</i>	Indicates the offset of changed metric values. The value is in the range from 0 to 16.
	<i>interface-type</i>	Applies the ACL to a specified interface.
	<i>interface-number</i>	Specifies the interface number.
Defaults	No offset is specified by default.	
Command Mode	Routing process configuration mode	
Usage Guide	If a RIP route matches against both the offset-list of the specified interface and the global offset-list, it will increase the metric value of the offset-list of the specified interface.	
Configuration Examples	The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7. <pre>FS (config-router)# offset-list 7 out 7</pre> The following example increases the metric of the RIP routes by 7 in the range specified by ACL 7 and learned by fastethernet 0/1. <pre>FS (config-router)# offset-list 8 in 7 fastethernet 0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.31 output-delay

	Use this command to modify the delay to send RIP update packets. Use the no form of this command to restore the default setting.	
	output-delay <i>delay</i>	
	no output-delay	
Parameter Description	Parameter	Description
	<i>delay</i>	Sets the delay to send RIP update packets, in the range from 8 to 50 in the unit of milliseconds.
Defaults	No sending delay is configured by default.	
Command Mode	Routing process configuration mode	

Usage Guide	In normal cases, the size of a RIP update packet is 512 bytes including 25 routes. If the number of updated routes is greater than 25, update packets will be sent through multiple routes. Note that the update packets should be sent as fast as possible. However, when a high-speed device sends a large number of packets to a low-speed device, the low-speed device may not process all the packets timely, resulting in packet loss. In this case, you can use this command to increase the delay to send packets on the high-speed device so that the low-speed device can process all the update packets.	
Configuration Examples	The following example sets the delay to send RIP update packets to 30 milliseconds. <pre>FS(config)# router rip FS(config-router)# output-delay 30</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.32 passive-interface

	Use this command to disable the function of sending update packets on an interface. Use the no form of this command to restore the default setting.	
	passive-interface { default <i>interface-type interface-num</i> }	
	no passive-interface { default <i>interface-type interface-num</i> }	
Parameter Description	Parameter	Description
	default	Sets all interfaces to the passive interfaces.
	<i>interface-type interface-num</i>	Indicates the interface type and number.
Defaults	Interfaces are set to the non passive interfaces by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The passive-interface default command sets all interfaces to the passive interfaces. You can use no passive-interface interface-type interface-num command to set specified interfaces as non-passive interfaces. After you set an interface to the passive interface, RIP route update packets will no longer be sent but can be received through the interface. In this case, route update packets can be sent to a specified neighbor through the interfaces by using the neighbor command. You can use the ip rip send enable and ip rip receive enable commands to control whether route update packets can be sent or received through the interface.	

Configuration Examples	The following example sets all interfaces to the passive interfaces and then sets ethernet0/1 to the non-passive interface.	
	<pre>FS(config-router)# passive-interface default FS(config-router)# no passive-interface gigabitEthernet 0/1</pre>	
Related Commands	Command	Description
	ip rip receive enable	Enables or disables receiving RIP packets on the interface.
	ip rip send enable	Enables or disables sending RIP packets on the interface.
Platform Description	N/A	

1.33 redistribute

	Use this command to redistribute external routes in route configuration mode. Use the no form of this command to restore the default setting.	
	redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> static } [{ level-1 level-1-2 level-2 }] [match { internal external [1 2] nssa-external [1 2] }] [metric <i>metric-value</i>] [route-map <i>route-map-name</i>]	
	no redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> static } [{ level-1 level-1-2 level-2 }] [match { internal external [1 2] nssa-external [1 2] }] [metric <i>metric-value</i>] [route-map <i>route-map-name</i>]	
Parameter Description	Parameter	Description
	bgp	Is redistributed from bgp.
	connected	Is redistributed from a connected route.
	isis <i>area-tag</i>	Is redistributed from ISIS and specifies an ISIS instance through area-tag.
	ospf <i>process-id</i>	Is redistributed from OSPF and specifies an OSPF instance through process-id. The value is in the range from 1 to 65535.
	static	Is redistributed from static routes.
	level-1 level-1-2 level-2	Is used when ISIS route redistribution is configured and specifies a route with a specific level for redistribution.
	match	Is used when OSPF route redistribution is configured and filters a route with a specific level for redistribution.
	metric <i>metric-value</i>	Sets the metric value of the redistributed route and specifies the metric value by using the metric-value parameter. The value is in the range from 1 to 16.
	route-map <i>route-map-name</i>	Sets the redistribution filtering rule.
Defaults	By default: All the routes of the sub types of the instance are redistributed when you configure redistributing OSPF. The routes of Level-2 sub-types of the instance are redistributed when you configure ISIS redistribution. All the routes of the protocol are redistributed for other routing protocols.	

	The metric of the redistributed routes is 1 by default. The route-map is not associated.	
Command Mode	Routing process configuration mode	
Usage Guide	This command is executed to redistribute external routes to RIP. It is unnecessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. For RIP, the metric value is calculated based on hop counts; for OSPF, the metric value is calculated based on bandwidths. Therefore, their metrics are not comparable. However, a symbolic metric value must be set for route redistribution. Otherwise, route redistribution will fail. When you configure ISIS route redistribution without the level parameter, only level-2 routes are redistributed by default. If the redistribution configuration is initialized with the level parameter, then all routes with level configured are redistributed. When the configuration is saved and level 1 and level 2 are configured at the same time, level 1 and level 2 are combined into the level-1-2 parameter to be saved. When you configure redistribution of OSPF routes without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. The no form of this command restores the setting to the default value. The rule of configuring the no form of the redistribute command is as follows: 1. If the no form of this command specifies certain parameters, the parameters must be restored to the default configuration. 2. If the no form of this command does not specify any parameter, the command must be deleted. Assume that the following configurations are available. <pre>redistribute isis 112 level-2</pre> You can use the no redistribute isis 112 level-2 command to modify the configuration. According to the preceding rule, this command only restores the level-2 parameter to the default value. However, level-2 is also the default parameter value. Therefore, the configuration is still be saved as redistribute isis 112 level-2 after you use the no form of this command. To delete this command, use the following command: <pre>no redistribute isis 112</pre>  The redistribute command cannot redistribute the default route of other protocol to the RIP process. To this end, use the default-information originate command.	
Configuration Examples	The following example redistributes static routes to RIP. <pre>FS(config-router)# redistribute static</pre>	
Related Commands	Command	Description
	default-metric <i>metric</i>	Sets the default metric of the route to be redistributed.
	default-information originate	Generates the default route in the RIP process.

Platform	N/A
Description	

1.34 router rip

	Use this command to create the RIP routing process and enter the routing process configuration mode. Use the no form of this command to restore the default setting.	
	router rip	
	no router rip	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No RIP process is running by default.	
Command Mode	Global configuration mode	
Usage Guide	One RIP routing process must be defined with one network number. If a dynamic routing protocol runs on asynchronous lines, configure the async default routing command on the asynchronous interface.	
Configuration Examples	The following example creates the RIP routing process and enters the routing process configuration mode. FS (config)# router rip FS(config-router)#	
Related Commands	Command	Description
	network (RIP)	Defines the network number of the RIP process.
Platform	N/A	
Description		

1.35 show ip rip

	Use this command to display the RIP process information.	
	show ip rip [vrf vrf-name]	
Parameter Description	Parameter	Description
	vrf vrf-name	(Optional) Displays the RIP information with the specified VRF.
Defaults	N/A	

Command	
Mode	Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode
Usage Guide	It is used to display the three timers, routing distribution status, routing re-distribution status, interface RIP version, RIP interface and network range, metric, and distance of the RIP process quickly. If the VRF is specified, the name of VRF and VRF ID are displayed.
Configuration Examples	The following example displays the basic information of the RIP process such as the update time and management distance. <pre> FS#show ip rip Routing Protocol is "rip" Sending updates every 10 seconds, Invalid after 20 seconds, flushed after 10 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not set Default redistribution metric is 2 Redistributing: connected Default version control: send version 2, receive version 2 Interface Send Recv FastEthernet 0/1 2 2 FastEthernet 0/2 2 2 Routing for Networks: 192.168.26.0 255.255.255.0 192.168.64.0 255.255.255.0 Distance: (default is 50) Graceful-restart enabled Restart grace period 60 secs Current Restart remaining time 16 secs </pre> The following example specifies the VRF and displays the corresponding basic information of RIP instance. <pre> FS(config-router)# sh ip rip vrf 1 VRF 1 VRF-id:1 Routing Protocol is "rip" Sending updates every 30 seconds, next due in 4 seconds Invalid after 180 seconds, flushed after 120 seconds Outgoing update filter list for all interface is: not set Incoming update filter list for all interface is: not set Default redistribution metric is 1 Redistributing: Default version control: send version 1, receive any version Routing for Networks: Distance: (default is 120) </pre>

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.36 show ip rip database

	Use this command to display the route summary information in the RIP routing database.	
	show ip rip database [vrf <i>vrf-name</i>] [<i>network-number network-mask</i>] [count]	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	(Optional) Displays the RIP routing information of specified VRF.
	<i>network-number</i>	(Optional) Indicates the ID of the subnet on which route information is to be displayed.
	<i>network-mask</i>	Indicates the subnet mask. It must be specified if the network number is specified.
	count	(Optional) Displays the abstract of the route statistics in the RIP database.
Command Mode	Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode	
Usage Guide	Only when the related sub-routes are converged, the converged address entries appear in the RIP routing database. When the last sub-route information in the converged address entries becomes invalid, the converged address information will be deleted from the database.	
Configuration Examples	The following example displays all converged address entries in the RIP routing database. <pre>FS# show ip rip database 192.168.1.0/24 auto-summary 192.168.1.0/30 directly connected, Loopback 3 192.168.1.8/30 directly connected, FastEthernet 0/1 192.168.121.0/24 auto-summary 192.168.121.0/24 redistributed [1] via 192.168.2.22, FastEthernet 0/2 192.168.122.0/24 auto-summary 192.168.122.0/24 [1] via 192.168.4.22, Serial 0/1 00:28 permanent</pre> The following example displays the converged address entries related with 192.168.121.0/24 in the RIP routing database. <pre>FS# show ip rip database 192.168.121.0 255.255.255.0 192.168.121.0/24 redistributed</pre>	

	[1] via 192.168.2.22, FastEthernet 0/1 The following example displays the statistical information summary of various routes in the RIP routing database. <pre>FS# show ip rip database count</pre> <table><thead><tr><th></th><th>All</th><th>Valid</th><th>Invalid</th></tr></thead><tbody><tr><td>database</td><td>5</td><td>5</td><td>0</td></tr><tr><td>auto-summary</td><td>5</td><td>5</td><td>0</td></tr><tr><td>connected</td><td>1</td><td>1</td><td>0</td></tr><tr><td>rip</td><td>4</td><td>4</td><td>0</td></tr></tbody></table>			All	Valid	Invalid	database	5	5	0	auto-summary	5	5	0	connected	1	1	0	rip	4	4	0
	All	Valid	Invalid																			
database	5	5	0																			
auto-summary	5	5	0																			
connected	1	1	0																			
rip	4	4	0																			
Related Commands	Command	Description																				
	show ip rip	Displays the information of the currently-running routing protocol process.																				
Platform Description	N/A																					

1.37 show ip rip external

	Use this command to display the information of the external routes redistributed by the RIP protocol.	
	<i>show ip rip external [bgp connected isis [process-id] ospf process-id static] [vrf vrf-name]</i>	
Parameter Description	Parameter	Description
	bgp	Displays redistributed BGP routes.
	connected	Displays redistributed directly-connected routes.
	isis process-id	Displays redistributed ISIS routes. The process-id parameter indicates ISIS process ID.
	ospf process-id	Displays redistributed OSPF routes. The process-id parameter indicates OSPF process ID. The range is from 1 to 65535.
	static	Displays redistributed static routes.
	vrf vrf-name	Displays the RIP external route of the specified VRF (optional).
Defaults	N/A	
Command Mode	Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays direct routes redistributed by the RIP process.	
	FS# show ip rip external	

	Protocol connected route: [connected] 192.100.3.0/24 metric=0 nhop=0.0.0.0, if=2 [connected] 192.101.1.0/24 metric=0 nhop=0.0.0.0, if=3 Protocol static route: [static] 10.1.1.1/32 metric=0 nhop=0.0.0.0, if=4096 [static] 10.1.2.1/32 metric=0 nhop=0.0.0.0, if=4096 Protocol ospf 1 route: [ospf] 1.1.1.1/32 metric=2 nhop=192.100.3.2, if=2 [ospf] 90.1.1.1/32 metric=2 nhop=192.100.3.2, if=2	
Related Commands	Command	Description
	show ip rip	Displays the information of the currently running routing protocol process.
	ip vrf	Creates a VRF.
Platform Description	N/A	

1.38 show ip rip interface

	Use this command to display the RIP interface information.	
	<i>show ip rip interface [vrf vrf-name] [interface-type interface-number]</i>	
Parameter Description	Parameter	Description
	vrf vrf-name	Displays the RIP interface of specified VRF (optional).
	[<i>interface-type</i> <i>interface-number</i>]	Displays the specified interface type and interface number (optional).
Defaults	N/A	
Command Mode	Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode	
Usage Guide	This command is used to display the information about RIP interfaces. If no RIP interface exists, no information is displayed.	

Configuration	The following example displays the RIP interface information.
Examples	<pre> FS# show ip rip interface FastEthernet 0/1 is up, line protocol is up Routing Protocol: RIP Receive RIPv2 packets only Send RIPv2 packets only Recv RIP packet total: 0 Send RIP packet total: 3 Passive interface: Disabled Split Horizon with Poisoned Reverse: Enabled Triggered RIP Enabled: Retransmit-timer: 5, Retransmit-count: 36 V2 Broadcast: Disabled Multicast registe: Registered Interface Summary Rip: Not Configured Authentication mode: Text Authentication key-chain: ripk1 Authentication text-password: FS Default-information: only, metric 5 IP interface address: 192.168.64.100/24, next update due in 14 seconds 2.2.1.1/24, next update due in 24 seconds neighbor 2.2.1.6, next update due in 3 seconds neighbor 2.2.1.77, next update due in 13 seconds 2.2.2.57/24, next update due in 16 seconds If the BFD has been configured for RIP, the BFD information is also displayed. FS#show ip rip interface Serial 0/1 is up, line protocol is up Routing Protocol: RIP Receive RIPv1 and RIPv2 packets Send RIPv1 packets only Receive RIP packet: Enabled Send RIP packet: Enabled Send RIP supernet routes: Enabled Recv RIP packet total: 0 Send RIP packet total: 3 Passive interface: Disabled Split Horizon: Enabled Triggered RIP Disabled BFD: Enabled V2 Broadcast: Disabled Multicast registe: Registered Interface Summary Rip: </pre>

	Not Configured IP interface address: 2.2.2.111/24, next update due in 14 seconds	
Related Commands	Command	Description
	show ip rip	Displays the information of the currently running routing protocol process.
Platform Description	N/A	

1.39 show ip rip peer

	Use this command to show the RIP peer information. RIP records a summary for the RIP routing information source learnt (source addresses of RIP route update packets) for the convenience of user monitoring. This routing information source is called RIP neighbor information.	
	show ip rip peer [<i>ip-address</i>] [vrf <i>vrf-name</i>]	
Parameter Description	Parameter	Description
	<i>ip-address</i>	(Optional) Displays the IP address of a specified RIP neighbor.
	vrf <i>vrf-name</i>	(Optional) Displays the RIP interface of a specified VRF.
Defaults	N/A	
Command Mode	Privileged EXEC mode/ Global configuration mode/ Routing process configuration mode	
Usage Guide	This command is used to display the RIP neighbor information. If no RIP neighbor exists, no information will be displayed.	
Configuration Examples	The following example displays the RIP neighbor information. <pre> FS# show ip rip peer Peer 192.168.3.2: Local address: 192.168.3.1 Input interface: GigabitEthernet 0/2 Peer version: RIPv1 Received bad packets: 3 Received bad routes: 0 BFD session state up </pre>	
Related Commands	Command	Description

	show ip rip	Displays the information of the routing protocol process that is running.
Platform Description	N/A	

1.40 timers basic

	Use this command to adjust the RIP clock. Use the no form of this command to restore the default setting.	
	timers basic <i>update invalid flush</i>	
	no timers basic	
Parameter Description	Parameter	Description
	update	Indicates the route update time in seconds. The update keyword defines the period at which the device sends route update packets. Each time an update packet is received, the "Invalid" and "Flush" clocks are reset. By default, a route update packet is sent every 30 seconds.
	invalid	Indicates the route invalid time in seconds, starting from the last valid update packet. The "invalid" defines the period when the route in the routing table becomes invalid due to no update. The invalid period of route shall be at least three times the route update period. If no update packet is received within the route invalid period, the related route becomes invalid and enters into the "invalid" state. If an update packet is received within the period, the clock resets. By default, the Invalid time is 180 seconds.
	flush	Indicates the route flushing time in seconds, starting when a RIP route enters into the invalid status. When the flush time is due, the routes in the invalid status will be cleared out of the routing table. The default Flush time is 120 seconds.
Defaults	By default, the update time is 30 seconds, the invalid time is 180 seconds, and the flushing time is 120 seconds.	
Command Mode	Routing process configuration mode	
Usage Guide	Adjusting the above clocks may speed up routing protocol convergence and fault recovery. Devices connected to the same network must have consistent RIP clock values. Adjustment of RIP clocks is not recommended unless otherwise specified. To check the current RIP clock parameters, use the show ip rip command.  If you set the clock to a small value on low-speed links, some risks will be caused because numerous update packets may use up the bandwidth. In general, the clocks can be configured with smaller values on Ethernet or the lines of above 2 Mbit/s to reduce the convergence time of routes.	

Configuration Examples	The following example enables the RIP update packets that are sent every 10 seconds. If no update packet is received within 30 seconds, related routes become invalid and enter the invalid status. When another 90s elapses, they will be cleared.	
	<pre>FS (config)# router rip FS (config-router)# timers basic 10 30 90</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.41 validate-update-source

	Use this command to validate the source address of the received RIP route update packet. Use the no form of the command to disable this function.	
	validate-update-source	
	no validate-update-source	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	You can validate the source address of the RIP route update packet. The validation aims to ensure that the RIP routing process receives only the route update packets from the same IP subnet neighbor. Disabling split horizon on the interface causes the RIP routing process to enable update message source address validation, no matter whether it has been configured with the validate-update-source command in routing process configuration mode. In addition, for the ip unnumbered interface, the RIP routing process does not implement update message source address validation, no matter whether it has been configured with the command validate-update-source.	
Configuration Examples	The following example disables verification of the source IP address of the update packet.	
	<pre>FS (config)# router rip FS (config-router)# no validate-update-source</pre>	
Related Commands	Command	Description
	ip split-horizon	Enables split horizon.

	ip unnumbered	Defines the IP unnumbered interface.
	neighbor (RIP)	Defines the IP address of a RIP neighbor.
Platform Description	N/A	

1.42 version

	Use this command to define the RIP version of a device. Use the no form of this command to restore the default setting.	
	version { 1 2 }	
	no version	
Parameter Description	Parameter	Description
	1	Defines the RIP version 1.
	2	Defines the RIP version 2.
Defaults	The route update packets of RIPv1 and are received by default, but only the RIPv1 route update packets are sent.	
Command Mode	Routing process configuration mode	
Usage Guide	This command defines the RIP version running on the device. It is possible to redefine the messages of which RIP version are processed on every interface by using the ip rip receive version and ip rip send version commands.	
Configuration Examples	The following example configures the RIP version as version 2. <pre>FS (config)# router rip FS (config-router)# version 2</pre>	
Related Commands	Command	Description
	ip rip receive version	Defines the version of RIP packets received on the interface.
	ip rip send version	Defines the version of RIP packets sent on the interface.
	show ip rip	Displays RIP information.
Platform Description	N/A	

2 OSPFv2 Commands

2.1 area

	Use this command to configure the specified OSPF area. Use the no form of this command to restore the default setting.	
	area <i>area-id</i>	
	no area <i>area-id</i>	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the OSPF area. The value can be a decimal integer or an IP address.
Defaults	No OSPF area is configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	Use the no form of this command to remove the specified OSPF area and its configuration, including the area-based area authentication, area default-cost, area filter-list, and area nssa commands. - Do not remove the OSPF area configuration under the following conditions: - Virtual links exist in the backbone area. The virtual links must be removed at first. - The corresponding network area command exists in any area. All network segment commands added to an area must be removed at first.	
Configuration Examples	The following example removes the configuration of OSPF area 2. <pre>FS(config)# router ospf 2 FS(config-router)# no area 2</pre>	
Related Commands	Command	Description
	network area	Defines the interface where OSPF runs and the belonging area of the interface.
Platform Description	N/A	

2.2 area authentication

	Use this command to enable OSPF area authentication. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> authentication [message-digest]	

	no area <i>area-id</i> authentication	
Parameter Description	Parameter	Description
	<i>area-id</i>	Specifies ID of the area enabled with OSPF. The value can be a decimal integer or an IP address.
	message-digest	(Optional) Enables MD5 (message digest 5) authentication mode.
Defaults	No authentication is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The FSOS software supports three authentication types: 1) 0, no authentication. The authentication type in the OSPF packet is 0 when this command is not executed to enable OSPF authentication. 2) 1, plain text authentication mode. When this command is configured, the message-digest option is not used. 3) 2, MD5 authentication mode. When this command is configured, the message-digest option is used. All devices in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication password must be configured on an interface connecting neighbors. You can use the ip ospf authentication-key command to configure the plain text authentication password, and the ip ospf message-digest-key command to configure the MD5 authentication password in interface configuration mode.	
Configuration Examples	The following example uses MD5 authentication and the authentication password backbone in area 0 (backbone area) of the OSPF routing process. <pre> FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone FS(config)# router ospf 1 FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 FS(config-router)# area 0 authentication message-digest </pre>	
Related Commands	Command	Description
	ip ospf authentication-key	Defines the OSPF plain text authentication password.
	ip ospf message-digest-key	Defines the OSPF MD5 authentication password.
	area virtual-link	Defines a virtual link.
Platform Description	N/A	

2.3 area default-cost

	Use this command to define the cost (OSPF metric) of the default aggregate route advertised to the stub area or not-so-stubby area (NSSA) in routing process configuration mode. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> default-cost <i>cost</i>	
	no area <i>area-id</i> default-cost	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the stub area or NSSA
	<i>cost</i>	Cost of the default aggregate route advertised to the stub area or NSSA. The range is from 0 to 16777215.
Defaults	The default is 1.	
Command Mode	Routing process configuration mode	
Usage Guide	This command takes effect only on the Area Border Router (ABR) of the stub area or the ABR/Autonomous System Border Router (ASBR) of the NSSA. The ABR can advertise a Link State Advertisement (LSA) indicating the default route in the stub area. The ABR/ASBR can advertise an LSA indicating the default route in the NSSA. You can use the area default-cost command to modify the LSA cost.	
Configuration Examples	The following example sets the cost of the default aggregate route to 50. <pre> FS(config)# router ospf 1 FS(config-router)# network 172.16.0.0 0.0.255.255 area 0 FS(config-router)# network 192.168.12.0 0.0.0.255 area 1 FS(config-router)# area 1 stub FS(config-router)# area 1 default-cost 50 </pre>	
Related Commands	Command	Description
	area stub	Sets an OSPF area as a stub area.
	area nssa	Sets an OSPF area as an NSSA.
Platform Description	N/A	

2.4 area filter-list

	Use this command to filter the inter-area routes on the ABR. Use the no form of this command to restore the default setting.

	area <i>area-id</i> filter-list { access <i>acl-name</i> prefix <i>prefix-name</i> } { in out }	
	no area <i>area-id</i> filter-list { access <i>acl-name</i> prefix <i>prefix-name</i> } { in out }	
Parameter Description	Parameter	Description
	<i>area-id</i>	Area ID
	<i>acl-name</i>	Name of an Access Control List (ACL)
	<i>prefix-name</i>	Prefix-list name
	in out	Applies the ACL rule to the routes incoming/outgoing the area.
Defaults	No filtering is configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	This command can be configured only on an ABR. You can use this command when it is required to filter the inter-area routes on the ABR.	
Configuration Examples	The following example sets area 1 to learn only the inter-area routes of 172.22.0.0/8. <pre> FS# configure terminal FS(config)# access-list 1 permit 172.22.0.0 0.255.255.255 FS(config)# router ospf 100 FS(config-router)# area 1 filter-list access 1 in </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.5 area nssa

	Use this command to set an OSPF area as an NSSA in routing process configuration mode. Use the no form of this command to delete the NSSA or the NSSA configuration.	
	area <i>area-id</i> nssa [no-redistribution] [default-information-originate [metric <i>value</i>] [metric-type <i>type</i>]] [no-summary] [translator [stability-interval <i>seconds</i> always]]	
	no area <i>area-id</i> nssa [no-redistribution] [default-information-originate [metric <i>value</i>] [metric-type <i>type</i>]] [no-summary] [translator [stability-interval always]]	
Parameter Description	Parameter	Description
	<i>area-id</i>	NSSAID
	no-redistribution	Imports the routing information to a common area other than the

		NSSA for the NSSA ABR.
	default-information originate	Generates and imports the default Type 7 LSA to the NSSA. This option takes effect only on the NSSA ABR or ASBR.
	metric <i>value</i>	Sets the metric of the generated default LSA. The range is from 0 to 16777214. The default value is 1.
	metric-type <i>type</i>	Sets the type of the generated LSA to N-1 or N-2. The default value is N-2.
	no-summary	Prevents the NSSA ABR from sending summary LSAs (Type-3 LSA).
	translator	Configures the translator for the NSSA ABR.
	stability-interval <i>seconds</i>	Configures the stability interval in seconds for the NSSA ABR that functions as a translator to change to a non-translator. The range is from 0 to 2147483647. The default value is 40.
	always	Configures that an NSSA ABR always functions as a translator. The NSSA ABR is the backup translator by default.
Defaults	No NSSA is defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The default-information-originate parameter is used to generate the default Type-7 LSA. However, on the NSSA ABR, the default Type-7 LSA will always be generated; On the ASBR (which is not an ABR at the same time), the default Type-7 LSA is generated only when the default route exists in the routing table. The no-redistribution parameter prevents the OSPF from advertising the external routes imported with the redistribute command to the NSSA on the ASBR. This option is generally used when the NSSA device is both an ASBR and an ABR. To reduce the number of LSAs sent to the NSSA, you can configure the no-summary parameter on the ABR to prevent it from advertising summary LSAs (Type-3 LSAs) to the NSSA. In addition, you can use the area default-cost command on the NSSA ABR to configure the cost of the default route advertised to the NSSA. By default, this cost is 1. If an NSSA has multiple ABRs, the ABR with the greatest ID is selected as the Type-7 or Type-5 translator. To configure that an NSSA ABR always functions as a translator, you can use the translator always parameter. If the translator role of an ABR is taken away by another ABR, the ABR still possesses the conversion capability within stability-interval. If the ABR fails to take back its translator role when stability-interval expires, the LSA that changes from Type-7 to Type-5 will be removed from the autonomous domain. To avoid route loops, Type-5 LSAs generated from Type-7 convergence will be eliminated immediately after the current device stopped serving as a translator, with no need to wait until the stability-interval expires. In a same NSSA, you are recommended to configure the translator always parameter on only one ABR.	
Configuration Examples	The following example sets area 1 as an NSSA on all routers of the area. <pre> FS(config)#router ospf1 FS(config-router)#network 172.16.0.0.0.255.255 area0 FS (config-router)#network 192.168.12.0.0.0.255 area 1 FS(config-router)# area1nssa </pre>	

Related Commands	Command	Description
	area default-cost	Defines the cost (OSPF metric) of the default aggregate route advertised to the NSSA.
Platform Description	N/A	

2.6 area range

	Use this command to configure inter-area route aggregation for OSPF. Use the no form of this command to delete route aggregation. Use the no form with the cost parameter to restore the default metric of the aggregate route, but not delete route aggregation.	
	area <i>area-id</i> range <i>ip-address net-mask</i> [advertise not-advertise] [cost <i>cost</i>]	
	no area <i>area-id</i> range <i>ip-address net-mask</i> [<i>cost</i>]	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the area where the aggregate route is injected into. The value can be a decimal integer or an IP address.
	<i>ip address net-mask</i>	Network segment whose routes are to be aggregated
	advertise not-advertise	Whether to advertise the aggregate route
	cost <i>cost</i>	Sets the priority of the interface. The range is from 0 to 16777215.
Defaults	No inter-area route aggregation is configured by default. The configured aggregation range is advertised by default. The default metric of the aggregate route depends on whether the device is compatible with RFC1583. If yes, the default metric is the smallest cost of the aggregate route. If no, the default metric is the largest cost of the aggregate route.	
Command Mode	Routing process configuration mode	
Usage Guide	This command takes effect only on the ABR to aggregate multiple routes of an area into a route and advertise it to other areas. Route combination occurs only on the border of an area. The devices inside an area see the specific routing information, but the devices outside the area see only one aggregate route. The advertise and not-advertise options can set whether to advertise the aggregate route for filtering and masking. The aggregate route is advertised by default. You can use the cost option to set the metric of the aggregate route. You can define route aggregate in multiple areas to simplify the routes in the whole OSPF routing area. This improves the network forwarding performance, especially in large networks. The area range of route aggregation is determined according to the longest match when multiple aggregate routes with direct inclusion relationships are configured.	

Configuration	The following example aggregate the routes of area 1 into a route 172.16.16.0/20.	
Examples	<pre>FS(config)#router ospf 1 FS(config-router)#network 172.16.0.0 0.15.255 area0 FS((config-router)#network 172.16.17.0 0.15.255 area1 FS(config-router)#area1 range 172.16.16.0 255.255.240.0</pre>	
Related Commands	Command	Description
	discard-route	Enables a discarded route to be added to a routing table.
	summary-address	Configures the OSPF external route aggregation.
Platform Description	N/A	

2.7 area stub

	Use this command to set an OSPF area as a stub area or full stub area. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> stub [no-summary]	
	no area <i>area-id</i> stub [no-summary]	
Parameter Description	Parameter	Description
	<i>area-id</i>	Stub area ID
	no-summary	(Optional) Prevents the ABR from advertising the network summary link to the stub area. Here the stub area is called the full stub area. Only the ABR needs this parameter.
Defaults	No stub area is defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	All devices in the OSPF stub area must be configured with the area stub command. The ABR only sends three types of link state advertisement (LSA) to the stub area: 1) type 1, device LSA; 2) type 2, network LSA; 3) type 3, network summary LSA. For the routing table, the devices in the stub area can learn only the routes inside the OSPF routing domain, including the internal default routes generated by the ABR. To configure a full stub area, use the area stub command with the no-summary keyword on the ABR. The devices in the full stub area can learn only the routes in the local area and the internal default routes generated by the ABR. Two commands can configure an OSPF area as a stub area: the area stub and area default-cost commands. All devices connected to the stub area must be configured with the area stub command, but the area default-cost	

	command can be executed only on the ABR. The area default-cost command defines the initial cost (metric) of the internal default route.	
Configuration Examples	The following example sets area 1 as the stub area on all devices in area 1. <pre>FS(config)# router ospf1 FS(config-router)# network 172.16.0.0 0.0.255.255 area 0 FS(config-router)# network 192.168.12.0 0.0.0.255 area 1 FS(config-router)# area 1 stub</pre>	
Related Commands	Command	Description
	area default-cost	Defines the cost (OSPF metric value) of the default aggregate route advertised to the stub area.
Platform Description	N/A	

2.8 area virtual-link

	Use this command to define the OSPF virtual link in routing process configuration mode. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> virtual-link <i>router-id</i> [authentication [message-digest null]] [dead-interval { <i>seconds</i> minimal } hello-multiplier <i>multiplier</i>] [hello-interval <i>seconds</i>] [retransmit-interval <i>seconds</i>] [transmit-delay <i>seconds</i>] [[authentication-key [<i>0 7</i>] <i>key</i>] [message-digest-key <i>key-id</i> <i>md5</i> [<i>0 7</i>] <i>key</i>]]	
	no area <i>area-id</i> virtual-link <i>router-id</i> [authentication] [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay] [[authentication-key] [message-digest-key <i>key-id</i>]]	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the OSPF transition area. The value can be a decimal integer or an IP address.
	<i>router-id</i>	ID of the router neighboring to the virtual link. It can be viewed with the show ip ospf command.
	dead-interval <i>seconds</i>	(Optional) Defines the time to declare neighbor loss in seconds. The range is 0 to 2147483647. This value must be consistent with that of the neighbor.
	minimal	Enables the Fast Hello function and sets the death clock to 1 second.
	hello-multiplier	Multiplies dead-interval with hello-interval in the Fast-Hello function.
	<i>multiplier</i>	Specifies the number of Hello packets that are sent every second in the Fast Hello function. The range is from 3 to 20.
	hello-interval <i>seconds</i>	(Optional) Defines the interval at which the HELLO packet is sent by the OSPF to the virtual link in seconds. The range is from 1 to 65535. This value must be consistent with that of the neighbor.
	retransmit-interval <i>seconds</i>	(Optional) OSPF LSA retransmission interval in seconds. The range is from 0 to

		65535. The parameter setting must consider the round-trip time of packets on the link.
	transmit-delay <i>seconds</i>	(Optional) OSPF LSA transmission delay in seconds. The range is from 0 to 65535. This value adds the LSA keep alive period. When the LSA keep alive period reaches a threshold, the LSA will be refreshed.
	authentication-key [0 7] <i>key</i>	(Optional) Defines the OSPF plain text authentication key. The plain text authentication key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
	message-digest-key <i>key-id</i> md5 [0 7] <i>key</i>	(Optional) Defines the OSPF MD5 authentication key and key ID. The MD5 authentication key ID and key between neighbors must be the same. The service password-encryption command enables the key to be displayed in encrypted manner. 0 indicates that the key is displayed in plain text. 7 indicates that the key is displayed in cipher text.
	authentication	Sets the authentication type to plain text.
	message-digest	Sets the authentication type to MD5.
	null	Sets the authentication type to no authentication.
Defaults	The following are the default values: dead-interval: 40seconds hello-interval: 10seconds retransmit-interval: 5seconds transmit-delay: 1second authentication: null The Fast Hello function is disabled by default. The other parameters do not have default values.	
Command Mode	Routing process configuration mode	
Usage Guide	A virtual link can connect an area to the backbone area, or another non-backbone area. In the OSPF routing domain, all areas must connect to the backbone area. If an area disconnects from the backbone area, a virtual link to the backbone area is required. Otherwise, the network communication will become abnormal. The virtual link is created between two ABRs. The area that belongs to both ABRs is called the transition area, which can never be a stub area or NSSA. The router-id parameter indicates the ID of OSPF neighbor router and can be displayed with the show ip ospf neighbor command. You can configure the loopback address as the router ID. The area virtual-link command defines only the authentication key for a virtual link. You can use the area authentication command to enable the OSPF packet authentication in areas connected over the virtual link in routing process configuration mode. OSPF supports the Fast Hello function.	

	If the Fast Hello function is enabled, the OSPF can discover neighbors and detects invalid neighbors quickly. You can enable the OSPF Fast Hello function by specifying the keywords minimal and hello-multiplier, and the multiplier parameter. You can set the death clock to 1 second in minimal and hello-multiplier to a value equal to or greater than 2. In this case, the Hello packet sending interval is less than 1 second. The hello-interval field of a Hello packet received by a virtual link is omitted if the Fast Hello function is enabled on the virtual link and the hello-interval field is set to 0 for Hello packets advertised from the virtual link. No matter the Fast Hello function is enabled or not, the values of dead-interval must be consistent on both ends of a virtual link. The values of hello-multiplier on both ends can be different if at least one Hello packet can be received within dead-interval. You can use the show ip ospf virtual-links command to monitor dead-interval and hello-interval configured for a virtual link. For the Fast Hello function, you can only configure either the dead-interval minimal hello-multiplier parameter or the hello-interval parameter.	
Configuration Examples	The following example sets area 1 as the transition area to establish virtual link with neighbor 2.2.2.2. <pre>FS(config)# router ospf 1 FS(config-router)# network 172.16.0.0.0.15.255 area0 FS(config-router)# network 172.16.17.0.0.15.255 area1 FS(config-router)# area1 virtual-link 2.2.2.2</pre>	
	The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1. This virtual link connects area 10 and the backbone area, and works with the OSPF packet authentication in MD5 mode. <pre>FS(config)# router ospf 1 FS(config-router)# network 172.16.17.0.0.15.255 area1 FS(config-router)# network 172.16.252.0.0.0.255 area10 FS(config-router)# area 0 authentication message-digest FS(config-router)# area1 virtual-link 1.1.1.1 message-digest-key 1 md5 hello</pre> The following example sets area 1 as the transition area to establish a virtual link with neighbor 1.1.1.1, enables the Fast Hello function on this virtual link, and sets the multiplier to 3. <pre>FS(config)# router ospf 1 FS(config-router)# network 172.16.17.0.0.15.255 area1 FS(config-router)# network 172.16.252.0.0.0.255 area10 FS(config-router)# area1 virtual-link 1.1.1.1 dead-interval minimal hello-multiplier 3</pre>	
Related Commands	Command	Description
	area authentication	Enables the OSPF area packet authentication and define the authentication mode.
	show ip ospf	Displays the OSPF process information, including the router ID.
	show ip ospf virtual-links	Monitors information about a virtual link.
Platform Description	N/A	

2.9 auto-cost

	Use this command to enable the auto-cost function and set the reference bandwidth according to the reference bandwidth. Use the no form of this command to restore the default setting.	
	auto-cost [reference-bandwidth <i>ref-bw</i>]	
	no auto-cost [reference-bandwidth]	
Parameter Description	Parameter	Description
	<i>ref-bw</i>	Reference bandwidth, in the range from 1 to 4294967 Mbps.
Defaults	The default is 100Mbps.	
Command Mode	Routing process configuration mode	
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the auto-cost command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the bandwidth command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the ip ospf cost command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.	
Configuration Examples	The following example configures the reference bandwidth as 10 Mbps. <pre>FS(config)# routerospf1 FS(config-router)# network 172.16.10.0 0.0.0.255 area 0 FS(config-router)# auto-cost reference-bandwidth 10</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information
	ip ospf cost	Sets the cost value of the OSPF interface.
	bandwidth	Sets the interface bandwidth. This setting does not affect data transmission rate.
Platform Description	N/A	

2.10 bdf all-interfaces

	Use this command to enable Bidirectional Forwarding Detection (BFD) on all OSPF interfaces. Use the no form of this command to restore the default setting.	
	bdf all-interfaces	
	no bdf all-interfaces	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	BDF is disabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	OSPF dynamically discovers the neighbors through Hello packets. With the BFD function enabled, one BFD session will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPF will converge with the network immediately. You can also use the ip ospf bfd [disable] command in interface configuration mode to enable or disable the BFD function on the specified interface, which takes precedence over the bdf all-interfaces command in routing process configuration mode.	
Configuration Examples	<pre>FS(config)# router ospf 1 FS(config-router)# bdf all-interfaces</pre>	
Related Commands	Command	Description
	router ospf	Creates the OSPF routing process and enters routing process configuration mode.
	ip ospf bfd]	Enables the specified interface running OSPF or disabling BFD for link detection.
Platform Description	N/A	

2.11 capability opaque

	Use this command to enable Opaque LSA. Use the no form of this command to disable this function.
	capability opaque
	no capability opaque

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Opaque LSA is enabled by default.	
Command Mode	Routing process configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example disables Opaque LSA capability. <pre>FS(config)# router ospf 1 FS(config-router)# no capability opaque</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the global configuration of OSPF.
Platform Description	N/A	

2.12 clear ip ospf process

	Use this command to clear and restart the OSPF instance.	
	clear ip ospf (process-id) process	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF instance ID. When the ID is specified, the command clears data related to the specified instance and restarts the OSPF instance. When no ID is specified, the command clears data related to all running OSPF instances and restarts all the running OSPF instances.
Defaults	The rule recommended in the RFC 1583 is used by default.	
Command Mode	Privileged EXEC mode	
Usage Guide	Resetting the entire OSPF process causes that all neighbors are re-established and OSPF is greatly affected. Therefore, you are prompted to confirm the execution for deliberation.	
Configuration	The following example clears data of OSPF instance 1 and restarts OSPF instance 1.	

Examples	FS#clearipospf1process	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.13 compatible rfc1583

	Use this command to determine the RFC 1583 or RFC 2328 rule for selecting the optimal route among route table several routes to the same destination out of the Autonomous System (AS).	
	compatible rfc1583	
	no compatible rfc1583	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The RFC 1583 rule is used by default.	
Command Mode	Routing process configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example determines the best route with the RFC 2328 rule. FS(config)# routerospf1 FS(config-router)# nocompatible RFC1583	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information
Platform Description	N/A	

2.14 default-information originate

	Use this command to generate a default route to be injected into the OSPF routing domain in routing process configuration mode. Use the no form of this command to restore the default setting.	
	default-information originate [always] [metric <i>metric</i>] [metric-type <i>type</i>] [route-map <i>map-name</i>]	
	no default-information originate [always] [metric] [metric-type] [route-map <i>map-name</i>]	

Parameter Description	Parameter	Description
	always	(Optional) Generates the default route unconditionally, no matter whether the default route exists locally or not.
	metric <i>metric</i>	(Optional) Initial metric of the default route in the range from 0 to 16777214
	metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics on different devices; type 2, same metric on different devices. An external route of type 1 is more trustworthy than that of type 2.
	route-map <i>map-name</i>	Associated route map name. No route map is associated by default.
Defaults	No default route is generated by default. The default value of metric is 1. The default value of metric-type is 2.	
Command Mode	Routing process configuration mode	
Usage Guide	When the redistribute or default-information command is executed, the OSPF-enabled device automatically turns into the ASBR. The ASBR cannot generate the default route automatically or advertise it to all the devices in the OSPF routing domain. The ASBR can generate the default route with the default-information originate command in routing process configuration mode. If the always parameter is used, the OSPF routing process advertises an external default route to neighbors, no matter the default route exists or not. However, the local device does not display the default route. To make sure whether the default route is generated, use the show ip ospf database command to display the OSPF link state database. The external link identified with 0.0.0.0 indicates the default route. You can use the show ip route command on the OSPF neighbor to display the default route. The metric of the external default route can be defined only with the default-information originate command. There are two types of OSPF external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, the type 1 route takes precedence over the type 2 route. As a result, the show ip route command displays only the type 1 route. This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the area nssa default-information-originate command. The routers in the stub area cannot generate external default routes.  The range of set metric is 0 to 16777214 for the associated route map. If the value exceeds the range, introducing a route fails.	
Configuration Examples	The following example configures that OSPF generates an external default route and injects it to the OSPF routing domain. The default route is of type 1 and the metric 50. <pre>FS(config)#routerospf 1 FS(config-router)#network 172.16.24.0 0.0.0.255 area 0</pre>	

	FS(config-router)#default-information originate always metric 50 metric-type 1	
Related Commands	Command	Description
	show ip ospf database	Displays OSPF link state database.
	show ip route	Displays the IP route table.
	redistribute	Redistributes routes of other routing processes.
Platform Description	N/A	

2.15 default-metric

	Use this command to set the default metric of OSPF redistribution route. Use the no form of this command to restore the default setting.	
	default-metric <i>metric</i>	
	no default-metric	
Parameter Description	Parameter	Description
	<i>metric</i>	Default metric of the OSPF redistribution route in the range from 1 to 16777214
Defaults	The default metric is not configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The default-metric command must work with the redistribute command in routing process configuration mode to modify the initial metric of all redistributed routes. The configuration result of the default-metric command does not take effect for the external routes injected into the OSPF routing domain with the default-information originate command.	
Configuration Examples	The following example configures the default metric of the OSPF redistribution route as 50. <pre>Switch(config)# router rip FS(config-router)# network 192.168.12.0 Switch(config-router)# version 2 FS(config-router)# exit FS(config)# router ospf 1 FS(config-router)# network 172.16.10.0 0.0.0.255 area 0 Switch(config-router)# default-metric 50 FS(config-router)# redistribute rip subnets</pre>	

Related Commands	Command	Description
	redistribute	Redistributes the routes of other routing processes.
	show ip ospf	Displays the OSPF global configuration information.
Platform Description	N/A	

2.16 discard-route

	Use this command to enable adding the discard-route into the core route table. Use the no form of this command to disable this function.	
	discard-route { internal external }	
	no discard-route { internal external }	
Parameter Description	Parameter	Description
	internal	Enables adding the discard-route generated with the area range command
	external	Enables adding the discard-route generated with the summary-address command.
Defaults	Adding the discard-route is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	After route aggregation, the range may exceed the actual network range of the route table, and sending the data to the nonexistent network may cause loops or increase router loads. To prevent this situation, the discard-route is added to the route table on the ABR or the ASBR. The discard-route is generated automatically and will not be transmitted.	
Configuration Examples	The following example disables adding the discard routes generated with the area range command. <pre>FS(config)# router ospf 1 FS(config-router)# no discard-route internal</pre>	
Related Commands	Command	Description
	area range	Configures the route aggregation between OSPF areas.
	summary-address	Configures the route aggregation out of the OSPF routing domain.
Platform Description	N/A	

2.17 distance ospf

	Use this command to set the Administration Distance (AD) of different types of OSPF routes. Use the no form of this command to restore the default setting.	
	distance { <i>distance</i> ospf { [intra-area <i>distance</i>] [inter-area <i>distance</i> [route-map <i>map-name</i>]] [external <i>distance</i>] }	
	no distance [ospf]	
Parameter Description	Parameter	Description
	<i>distance</i>	Sets the route AD in the range from 1 to 255.
	intra-area <i>distance</i>	Sets the AD of the intra-area route in the range from 1 to 255.
	inter-area <i>distance</i>	Sets the AD of the inter-area route in the range from 1 to 255.
	External <i>distance</i>	Sets the AD of the external route in the range from 1 to 255.
Defaults	The default value is 110. The default intra-area distance is 110. The default inter-area distance is 110. The default external distance is 110.	
Command Mode	OSPF Routing process configuration mode	
Usage Guide	This command is used to specify different ADs for different types of OSPF routes.	
Configuration Examples	The following example sets the OSPF external route AD to 160. <pre>FS(config)# routerospf1 FS(config-router)# distance ospf external 160</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.18 distribute-list in

	Use this command to configure LSA filtering. Use the no form of this command to restore the default setting.	
	distribute-list { [<i>access-list-number</i> <i>name</i>] <i>prefix</i> <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>] route-map <i>route-map-name</i> } in [<i>interface-type</i> <i>interface-number</i>]	
	no distribute-list { [<i>access-list-number</i> <i>name</i>] <i>prefix</i> <i>prefix-list-name</i> [gateway <i>prefix-list-name</i>] <i>route-map</i> <i>route-map-name</i> } in [<i>interface-type</i> <i>interface-number</i>]	

Parameter Description	Parameter	Description
	<i>access-list-number</i> name	Uses the ACL filtering rule.
	gateway <i>prefix-list-name</i>	Uses the gateway filtering rule.
	Prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.
	route-map <i>route-map-name</i>	Uses the route-map filtering rule.
	<i>interface-type interface-number</i>	Configures the LSA route filtering on the interface.
Defaults	No filtering is configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the Shortest Path First (SPF) calculation to generate the corresponding routes. It does not affect the link status database or the route table of the neighbors. It only affects the routing entries calculated by local OSPF. This function is used to control routes that enter the ABR or ASBR. The following route-map rules will be supported if the route-map parameter is configured: match interface match ip address match ip address prefix-list match ip next-hop match ip next-hop prefix-list match metric match route-type match tag Filtering routes by using the distribute-list in command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the area filter-list or area range (containing the not-advertise parameter) command on the ABR to prevent generation of black-hole routes.	
Configuration Examples	The following example configures LSA filtering. <pre>FS(config)# access-list3 permit 172.16.0.0/24 FS(config)# router ospf 25 FS(config-router)# distribute-list 3 in ethernet 0/1</pre>	
Related Commands	Command	Description
	distribute-list out	Filters redistribution routes.
Platform Description	N/A	

2.19 distribute-list out

	Use this command to configure filtering redistribution routes. The function is similar to that of the redistribute command. Use the no form of this command to restore the default setting.	
	distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> } out [bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static]	
	no distribute-list { [<i>access-list-number</i> <i>name</i>] prefix <i>prefix-list-name</i> } out [bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static]	
Parameter Description	Parameter	Description
	<i>access-list-number</i> <i>name</i>	Uses the ACL filtering rule.
	prefix <i>prefix-list-name</i>	Uses the prefix-list filtering rule.
	bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static	Source of the routes to be filtered
Defaults	No filtering is configured by default.	
Command Mode	Routing process configuration mode	
Usage Guide	Similar to the redistribute route-map command, the distribute-list out command filters the routes that other protocols redistribute to the OSPF. However, the distribute-list out command does not redistribute routes by itself. It works with the redistribute command in most cases. The ACL filtering rule and the prefix-list filtering rule cannot coexist in the configuration, that is, the two rules cannot be configured at the same time for routes from the same source.	
Configuration Examples	The following example filters the redistributed static routes. <pre> FS(config)# routerospf1 FS(config)# redistribute static subnets FS(config-router)# distribute-list 22 outstatic FS(config-router)# distribute-list prefix jji out static % Access-list filter exists, please de-config first </pre>	
Related Commands	Command	Description
	distribute-list in	Configures LSA filtering.
	redistribute	Redistributes routes of other routing processes.
Platform Description	N/A	

2.20 enable mib-binding

	Use this command to bind the Management Information Base (MIB) with the specified OSPFv2 process. Use the no form of this command to restore the default setting.	
	enable mib-binding	
	no enable mib-binding	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The MIB is bound with the OSPFv2 process with the smallest ID by default.	
Command Mode	Routing process configuration mode	
Usage Guide	OSPFv2 MIB has no OSPFv2 process information, so the user operates a sole OSPFv2 process by SNMP. By default, OSPFv2 MIB is bound with the OSPFv2 process with the smallest ID. User operations take effect for this process. To operate the specified OSPF process over Simple Network Management Protocol(SNMP), use this command to bind the MIB to SNMP.	
Configuration Examples	The following example operates OSPFv2 process 100 over SNMP: <pre>FS(config)# routerospf100 FS(config-router)# enable mib-binding</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information.
	enable traps	Configures the OSPF TRAP function.
Platform Description	N/A	

2.21 enable traps

	The OSPFv2 process supports 16 kinds of TRAP packets, which are classified into four categories. Use this command to enable sending the specified TRAP messages. Use the no form of this command to restore the default setting.
	<pre>enable traps [error [IfAuthFailure IfConfigError IfRxBadPacket VrtIfAuthFailure VrtIfConfigError VrtIfRxBadPacket] Isa [LsdbApproachOverflow LsdbOverflow MaxAgeLsa OriginateLsa] retransmit [IfTxRetransmit VrtIfTxRetransmit] state-change [IfStateChange NbrRestartHelperStatusChange NbrStateChange NssaTranslatorStatusChange RestartStatusChange VrtIfStateChange VrtNbrRestartHelperStatusChange VrtNbrStateChange]]</pre>
	no enable traps [error [IfAuthFailure IfConfigError IfRxBadPacket VrtIfAuthFailure VrtIfConfigError

	VirtIfRxBadPacket] Isa [LsdbApproachOverflow LsdbOverflow MaxAgeLsa OriginateLsa] retransmit [IfTxRetransmit VirtIfTxRetransmit] state-change [IfStateChange NbrRestartHelperStatusChange NbrStateChange NssaTranslatorStatusChange RestartStatusChange VirtIfStateChange VirtNbrRestartHelperStatusChange VirtNbrStateChange]]																	
Parameter Description	Parameter	Description																
	error	Configures all traps switches related to errors. Use this parameter to set the following specified error traps switches. <table><tr><td>Ifauthfailure</td><td>Interface authentication error</td></tr><tr><td>Ifconfigerror</td><td>Interface parameter configuration error</td></tr><tr><td>Ifrxbadpacket</td><td>Error packets received on the interface</td></tr><tr><td>Virtifauthfailure</td><td>Authentication error on the virtual interface</td></tr><tr><td>Virtifconfigerror</td><td>Parameter configuration error on the virtual interface</td></tr><tr><td>Virtifrxbadpacket</td><td>Error packets received on the virtual interface</td></tr></table>	Ifauthfailure	Interface authentication error	Ifconfigerror	Interface parameter configuration error	Ifrxbadpacket	Error packets received on the interface	Virtifauthfailure	Authentication error on the virtual interface	Virtifconfigerror	Parameter configuration error on the virtual interface	Virtifrxbadpacket	Error packets received on the virtual interface				
Ifauthfailure	Interface authentication error																	
Ifconfigerror	Interface parameter configuration error																	
Ifrxbadpacket	Error packets received on the interface																	
Virtifauthfailure	Authentication error on the virtual interface																	
Virtifconfigerror	Parameter configuration error on the virtual interface																	
Virtifrxbadpacket	Error packets received on the virtual interface																	
	isa	Configures all traps switches related to the LSA. Use this parameter to set the following specified LSA traps switches. <table><tr><td>Lsdbapproachoverflow</td><td>External LSA count has reached the 90% of the upper limit.</td></tr><tr><td>Lsdboverflow</td><td>External LSA count has reached the upper limit.</td></tr><tr><td>Maxagelsa</td><td>LSA reaching the aging time</td></tr><tr><td>Originatelsa</td><td>Generates new LSA</td></tr></table>	Lsdbapproachoverflow	External LSA count has reached the 90% of the upper limit.	Lsdboverflow	External LSA count has reached the upper limit.	Maxagelsa	LSA reaching the aging time	Originatelsa	Generates new LSA								
Lsdbapproachoverflow	External LSA count has reached the 90% of the upper limit.																	
Lsdboverflow	External LSA count has reached the upper limit.																	
Maxagelsa	LSA reaching the aging time																	
Originatelsa	Generates new LSA																	
	retransmit	Configures all traps switches related to the retransmission. Use this parameter to set the following specified retransmit traps switches. <table><tr><td>Iftxretransmit</td><td>Packet retransmission on the interface</td></tr><tr><td>Virtiftxretransmit</td><td>Packet retransmission on the virtual interface</td></tr></table>	Iftxretransmit	Packet retransmission on the interface	Virtiftxretransmit	Packet retransmission on the virtual interface												
Iftxretransmit	Packet retransmission on the interface																	
Virtiftxretransmit	Packet retransmission on the virtual interface																	
	state-change	Configures all traps switches related to the state change. Use this parameter to set the following specified state-change switches. <table><tr><td>Ifstatechange</td><td>Interface state change</td></tr><tr><td>NbrRestartHelperStatusChange</td><td>State change during the neighbor GR process</td></tr><tr><td>Nbrstatechange</td><td>Neighbor state change</td></tr><tr><td>NssaTranslatorStatusChange</td><td>State change of the NSSA translator</td></tr><tr><td>RestartStatusChange</td><td>State change of the GR Restarter on the device</td></tr><tr><td>Virtifstatechange</td><td>State change on the virtual interface</td></tr><tr><td>VirtNbrRestartHelperStatusChange</td><td>Status change of the virtual neighbor GR process</td></tr><tr><td>Virtnbrstatechange</td><td>State change on the virtual neighbor</td></tr></table>	Ifstatechange	Interface state change	NbrRestartHelperStatusChange	State change during the neighbor GR process	Nbrstatechange	Neighbor state change	NssaTranslatorStatusChange	State change of the NSSA translator	RestartStatusChange	State change of the GR Restarter on the device	Virtifstatechange	State change on the virtual interface	VirtNbrRestartHelperStatusChange	Status change of the virtual neighbor GR process	Virtnbrstatechange	State change on the virtual neighbor
Ifstatechange	Interface state change																	
NbrRestartHelperStatusChange	State change during the neighbor GR process																	
Nbrstatechange	Neighbor state change																	
NssaTranslatorStatusChange	State change of the NSSA translator																	
RestartStatusChange	State change of the GR Restarter on the device																	
Virtifstatechange	State change on the virtual interface																	
VirtNbrRestartHelperStatusChange	Status change of the virtual neighbor GR process																	
Virtnbrstatechange	State change on the virtual neighbor																	
Defaults	All TRAP switches are disabled by default.																	

Command Mode	Routing process configuration mode	
Usage Guide	The snmp-server enable traps ospf command must be configured before you configure this command, for it is limited by the snmp-server command. This command is not limited by the binding of process and MIB, allowing to enable the TRAP switch for different processes simultaneously.	
Configuration Examples	The following example enables all TRAP switches of OSPFv2 process 100. <pre>FS(config)# routerospf100 FS(config-router)# enable traps</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information.
	enable mib-binding	Binds the OSPFv2 process with MIB.
	snmp-server enable traps ospf	Enables the OSPF TRAP notification function.
Platform Description	N/A	

2.22 fast-reroute

	Use this command to enable the OSPF FRR (Fast Reroute) function for the device. Use the no form of this command to restore the default setting.	
	fast-reroute { lfa downstream-paths route-map <i>route-map-name</i> }	
	no fast-reroute { lfa [downstream-paths] route-map } }	
Parameter Description	Parameter	Description
	lfa	Enables the LFA (loop-free alternate) path computation.
	downstream-paths	Enables the downstream path computation.
	route-map <i>route-map-name</i>	Specifies the backup path through the route map.
Defaults	The FRR function is disabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	If the lfa parameter is configured, computation of the loop-free standby path is enabled. In this case, you can use the interface mode command to specify the path protection mode of the interface. It is recommended that computation of the loop-free standby path be disabled if any of the following case exists on the network:	

	1. Virtual links exist. 2. Alternative ABRs exist. 3. An ASBR is also an ABR. 4. Multiple ABSRs advertise the same external route. If both lfa and downstream-paths are configured, computation of the downstream path is enabled. If route-map is configured, a standby path can be specified for a matched route through the route-map. When the OSPF fast reroute function is used, it is recommended that BFD be enabled at the same time so that the device can quickly detect any link failure and therefore shorten the forwarding interruption time. If the interface is up or down, to shorten the forwarding interruption time during OSPF fast reroute, you can configure carrier-delay 0 in L3 interface configuration mode to achieve the fastest switchover speed.					
Configuration Examples	The following example enables FRR for OSPF instance 1 and associates route map <i>fast-reroute</i>. <pre>FS(config)# route-map fast-reroute FS(config-route-map)# match ip address 1 FS(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1 backup-nexthop 192.168.1.2 FS(config)# router ospf 1 FS(config-router)# fast-reroute route-map fast-reroute</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>graceful-restart helper</td><td>Enables the OSPF graceful-restart helper.</td></tr></table>	Command	Description	graceful-restart helper	Enables the OSPF graceful-restart helper.	
Command	Description					
graceful-restart helper	Enables the OSPF graceful-restart helper.					
Platform Description	N/A					

2.23 graceful-restart

	Use this command to enable the graceful restart (GR) of OSPF on the device. Use the graceful-restart grace-period command to configure the grace period parameter and enable the OSPF GR function. Use the no form of this command to disable this function.	
	graceful-restart [grace-period <i>grace-period</i> inconsistent-lsa-checking]	
	no graceful-restart [graceful-period]	
Parameter Description	Parameter	Description
	grace-period <i>grace-period</i>	Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the graceperiod varies from 1s to 1800s. The default value is 120s.
	inconsistent-lsa-checking	Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence.After GR is enabled, topological change detection is enabled by default.
Defaults	This function is enabled by default.	

Command Mode	Routing process configuration mode	
Usage Guide	GR is configured based on the OSPF instance. Different instances could be configured with different parameters according to the actual situation. The graceful restart interval is the longest time between the OSPF restart and the graceful restart. In this period, you can perform link status reconstruction to restore the OSPF status to the original. With the interval times out, the OSPF will exit GR and perform common OSPF operations. The GR interval is 120 seconds set with the graceful-restart command, and the graceful-restart grace-period command allows you to change the interval explicitly. GR is unavailable when the Fast Hello function is enabled.	
Configuration Examples	The following example enables GR for the OSPF instance 1 and sets the restart interval for GR. <pre>FS(config)# router ospf 1 FS(config-router)# graceful-restart FS(config-router)# graceful-restart grace-period 60</pre>	
Related Commands	Command	Description
	graceful-restart helper	Enables the OSPF graceful-restart helper.
Platform Description	N/A	

2.24 graceful-restart helper

	Use this command to enable the graceful restart helper function. Use the no form of this command to restore the default setting.	
	graceful-restart helper disable	
	no graceful-restart helper disable	
	graceful-restart helper { strict-lsa-checking internal-lsa-checking }	
	no graceful-restart helper {strict-lsa-checking internal-lsa-checking }	
Parameter Description	Parameter	Description
	disable	Prohibits a device from acting as a GR helper for another device.
	strict-lsa-checking	Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
	internal-lsa-checking	Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.

Defaults	The GR helper is enabled by default. The router enabled with the GR helper does not check the LSA change by default.	
Command Mode	Routing process configuration mode	
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The disable option indicates that GR helper is not provided for any device that implements GR. After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure strict-lsa-checking to check Type 1 to 5 and Type 7 LSAs that indicate the network information or internal-lsa-checking to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (strict-lsa-checking and internal-lsa-checking) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.	
Configuration Examples	The following example disables the GF helper and modifies the policy of checking network changes. <pre>FS(config)# router ospf1 FS(config-router)# graceful-restart helper disable FS(config-router)# no graceful-restart helper disable FS(config-router)# graceful-restart helper strict-lsa-checking</pre>	
Related Commands	Command	Description
	graceful-restart	Enables GR on the device.
Platform Description	N/A	

2.25 ip ospf authentication

	Use this command to configure the authentication type. Use the no form of this command to restore the default setting.	
	ip ospf authentication [message-digest null]	
	no ip ospf authentication	
Parameter Description	Parameter	Description
	message-digest	Enables MD5 authentication on the interface.
	null	Enables no authentication.

Defaults	No authentication mode is configured and that of the local area is used on the interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	Plaintext authentication is applicable when no option is used with the command. Note that the no form of this command restores the default value. Whether authentication is used actually depends on authentication mode configured for the local area of the interface. If authentication mode is configured as null , no authentication is enabled. When both the interface and its area are configured with authentication, the one for the interface takes precedence.	
Configuration Examples	The following example configures MD5 authentication for OSPF on fastEthernet 0/1. <pre> FS (config)#interface fastEthernet0/1 FS(config-if-FastEthernet 0/1)# ipaddress172.16.1.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf authentication message-digest </pre>	
Related Commands	Command	Description
	area authentication	Enables authentication and defines authentication mode in the OSPF area.
	ip ospf authentication-key	Configures the plain text authentication key.
	ip ospf message-digest-key	Configures the MD5 authentication key.
Platform Description	N/A	

2.26 ip ospf authentication-key

	Use this command to configure the OSPF plain text authentication key in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf authentication-key [0 7] key	
	no ip ospf authentication-key	
Parameter Description	Parameter	Description
	0	Displays the key in plain text.
	7	Displays the key in cipher text.
	<i>key</i>	Key containing at most eight characters.
Defaults	It is disabled by default.	
Command	Interface configuration mode	

Mode		
Usage Guide	The ip ospf authentication-key command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighbor relationship cannot be established between two devices directly connected, and thus route information exchange is impossible. The keys may vary by interface, but the devices that are connected to the same physical network segment must use the same key. To enable the OSPF area authentication, execute the area authentication command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence.	
Configuration Examples	The following example configures the OSPF authentication key ospfauth for fast Ethernet 0/1. <pre>FS (config)#interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth</pre>	
Related Commands	Command	Description
	area authentication	Enables OSPF area authentication and defines authentication mode
	ip ospf authentication	Enables authentication on the interface and defines authentication mode
Platform Description	N/A	

2.27 ip ospf bfd

	Use this command to enable or disable the BFD on the specified OSPF interface. Use the no form of this command to restore the default setting.	
	ip rip bfd [disable]	
	no ip ospf bfd	
Parameter Description	Parameter	Description
	disable	Disables BFD on the specified OSPF interface.
Defaults	BFD is not configured by default, and the BFD configuration in OSPF process configuration mode shall prevail.	
Command Mode	Interface configuration mode	

Usage Guide	The interface-based configuration takes precedence over the bfd all-interfaces command used in process configuration mode. Based on the actual environment, you can run the ip ospf bfd command to enable BFD on a specified interface for link detection, or run the bfd all-interfaces command in OSPF process configuration mode to enable BFD on all interface of the OSPF process, or run the ospf bfd disable command to disable BFD on a specified interface.	
Configuration Examples	<pre>FS(config)# interface fastethernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf bfd</pre>	
Related Commands	Command	Description
	router ospf	Creates the OSPF routing process and enters routing process configuration mode.
	bfd all-interfaces	Enables the BFD on all OSPF interfaces.
Platform Description	N/A	

2.28 ip ospf cost

	Use this command to configure the cost (OSPF metric) of the OSPF interface for sending a packet in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf cost <i>cost</i>	
	no ip ospf cost	
Parameter Description	Parameter	Description
	<i>cost</i>	OSPF interface cost in the range from 0 to 65535
Defaults	The default interface cost is calculated as follows: Reference bandwidth/Bandwidth The reference bandwidth is 100 Mbps by default.	
Command Mode	Interface configuration mode	
Usage Guide	By default, the OSPF interface cost is 100Mbps/Bandwidth, where Bandwidth is the interface bandwidth configured with the bandwidth command in interface configuration mode. The default costs of different types of lines are as follows: ● 64K serial line: 1562 ● E1 line: 48	

	● 10M Ethernet: 10 ● 100M Ethernet: 1 The OSPF cost configured with the ip ospf cost command will overwrite the default configuration.						
Configuration Examples	The following example configures the OSPF cost of fastEthernet 0/1 to 100. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip ospf cost 100</pre>						
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>bandwidth</td><td>Specifies the interface bandwidth. This setting does not affect the data transmission rate.</td></tr><tr><td>show ip ospf</td><td>Displays the OSPF global configuration information</td></tr></table>	Command	Description	bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.	show ip ospf	Displays the OSPF global configuration information
Command	Description						
bandwidth	Specifies the interface bandwidth. This setting does not affect the data transmission rate.						
show ip ospf	Displays the OSPF global configuration information						
Platform Description	N/A						

2.29 ip ospf database-filter all out

	Use this command to stop advertising LSAs of an interface, that is, the LSA update packets are not sent on the interface. Use the no form of the command to restore the default setting.	
	ip ospf database-filter all out	
	no ip ospf database-filter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled and all LSA update packets can be sent on the interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	To stop sending LSA update packets on the interface, enable this function on the interface. Then, the device maintains the neighboring connections and accepts LSAs from neighbors, but stops sending LSAs to neighbors.	
Configuration Examples	The following example stops sending LSA update packets of fastEthernet 0/1. FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf database-filter all out	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.30 ip ospf dead-interval

	Use this command to configure the interval for determining the death of an interface neighbor in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf dead-interval { <i>seconds</i> minimal hello-multiplier <i>multiplier</i> }	
	no ip ospf dead-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Defines the interval for determining the neighbor death in seconds. The range is from 0 to 2,147,483,647.
	minimal	Indicates that the Fast Hello function is enabled to set the dead interval to 1s.
	hello-multiplier <i>multiplier</i>	Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.
Defaults	The value of dead-interval is 4 times the interval configured with the ip ospf hello-interval command by default.	
Command Mode	Interface configuration mode	
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record from the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment. OSPF supports the Fast Hello function. After the OSPF Fast Hello function is enabled, OSPF finds neighbors and detects neighbor failures faster. You can enable the OSPF Fast Hello function by specifying the minimal and hello-multiplier keywords and the multiplier parameter. The minimal keyword indicates that the death interval is set to 1s, and hello-multiplier indicates the number of Hello packets sent per second. In this way, the interval at which the Hello packet is sent decreases to less than 1s. If the Fast Hello function is configured for a virtual link, the Hello interval field of the Hello packet advertised on the virtual link is set to 0, and the Hello interval field of the Hello packet received on this virtual link is ignored. No matter whether the Fast Hello function is enabled, the death interval must be consistent and the	

	hello-multiplier values can be inconsistent on routers at both ends of the virtual link. Ensure that at least one Hello packet can be received within the death interval. Run the show ip ospf virtual-links command to monitor the death interval and Fast Hello interval configured for the virtual link. The dead-interval minimal hello-multiplier and hello-interval parameters introduced for the Fast Hello function cannot be configured simultaneously.	
Configuration Examples	The following example configures the interval for determining the death of the OSPF neighbor on fastEthernet 0/1 to30seconds. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf dead-interval30</pre>	
	The following example configures the value of hello-multiplier to3. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3</pre>	
Related Commands	Command	Description
	ip ospf hello-interval	Specifies the interval at which the OSPF sends Hello packets
	show ip ospf interface	Displays OSPF interface information.
Platform Description	N/A	

2.31 ip ospf disable all

	Use this command to prevent the specified interface from generating OSPF packets. Use the no form of this command to restore the default setting.	
	ip ospf disable all	
	no ip ospf disable all	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	OSPF packets are generated on the specified interface by default.	
Command Mode	Interface configuration mode	

Usage Guide	The interface configured with this command will ignore whether the network areas are matched. After this command is configured, an interface will not generate OSPF packets even if the interface belongs to the network; therefore, the interface does not receive or send any OSPF packets or participate in OSPF calculation.	
Configuration Examples	The following example prevents the specified interface from generating OSPF packets. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf disable all</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.32 ip ospf fast-reroute protection

	Use this command to specify the loop-free alternate (LFA) protection mode for an interface. Use the no form of this command to restore the default setting.	
	ip ospf fast-reroute protection { node link-node disable }	
	no ip ospf fast-reroute protection	
Parameter Description	Parameter	Description
	node	Enables LFA node protection.
	link-node	Enables LFA link node protection.
	disable	Disables LFA protection.
Defaults	LFA node protection is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Enabling the fast-reroute lfa command in OSPF process configuration mode will enable OSPF fast reroute and generate a backup route for the master route according to the specified LFA protection mode in interface configuration mode. By default, link protection is enabled on each OSPF interface. In this protection mode, the failure of a master link does not affect forwarding on the backup route. Use the node parameter to enable node protection for an interface, that is, the neighbor node of a master link does not affect forwarding on the backup route. Similarly, use the link-node parameter to protect the link and neighbor link of a master route at the same time. Use the disable parameter to disable the LFA protection function for an interface, that is, a backup entry is not generated for the routes with this interface as the next hop.	

Configuration Examples	The following example sets OSPF LFA fast reroute to link and node protection:	
	<pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf fast-reroute protection link-node</pre>	
Related Commands	Command	Description
	fast-reroute	Enables OSPF fast reroute.
Platform Description	N/A	

2.33 ip ospf fast-reroute no-eligible-backup

	Use this command in interface configuration mode to exclude an OSPF interface as a backup interface in OSPF fast reroute calculation. Use the no form of this command to restore the default setting.	
	ip ospf fast-reroute no-eligible-backup	
	no ip ospf fast-reroute no-eligible-backup	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	An OSPF interface can serve as a backup interface by default.	
Command Mode	Interface configuration mode	
Usage Guide	If the remaining bandwidth of an interface is small or if the interface and its active interface may fail at the same time, the interface cannot be used as a standby interface. Therefore, you need to run this command in interface configuration mode to prevent this interface from becoming a standby interface during OSPF fast reroute computation. After this command is executed, the standby interface is selected from other interface. This command does not take effect if fast-reroute route-map is configured.	
Configuration Examples	The following example excludes FastEthernet 0/1 as a backup interface in OSPF fast reroute calculation.	
	<pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf fast-reroute no-eligible-backup</pre>	
Related Commands	Command	Description
	fast-reroute	Enables OSPF fast reroute.

Platform Description	N/A

2.34 ip ospf hello-interval

	Use this command to set the interval for sending Hello packets in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf hello-interval <i>seconds</i>	
	no ip ospf hello-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for sending Hello packets in seconds. The range is from 1 to 65535.
Defaults	The defaults are as follows: 10seconds for Ethernet 10seconds for PPP or HDLC encapsulated interfaces 10seconds for frame relay PTP interfaces 30seconds for non-frame relay PTP sub-interface and X.25 interfaces	
Command Mode	Interface configuration mode	
Usage Guide	The interval of sending the Hello packets is included in the Hello packet. A shorter interval means that OSPF detects the topological change faster, which will increase network traffic. The Hello packet sending intervals for all the devices in the same network segment must be the same. To manually modify the interval to determine neighbor death, ensure that the Hello packet sending interval cannot be greater than dead-interval of the neighbor.	
Configuration Examples	The following example configures the interval of sending the Hello packets on fastEthernet 0/1 to 15. <pre> FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf hello-interval 15 </pre>	
Related Commands	Command	Description
	ip ospf dead-interval	Sets the interval for determining the death of the OSPF neighbor.
Platform Description	N/A	

2.35 ip ospf message-digest-key

	Use this command to configure the MD5 authentication key in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf message-digest-key <i>key-id</i> md5 [0 7] <i>key</i>	
	no ip ospf message-digest-key <i>key-id</i>	
Parameter Description	Parameter	Description
	<i>key</i>	Key of up to 16 characters
	0	Displays the key in plain text.
	7	Displays the key in cipher text.
	<i>key-id</i>	Key identifier in the range from 1 to 255
Defaults	No MD5 key is configured by default.	
Command Mode	Interface configuration mode	
Usage Guide	The ip ospf message-digest-key command configures the key that will be inserted in all OSPF packet headers. As a result, if the keys are inconsistent, the OSPF neighboring relationship cannot be established between two devices directly connected, and thus route information exchange is impossible. The keys can be different for different interfaces, but the devices that are connected to the same physical network segment must be configured with the same key. For neighbors, the same key identifier must correspond to the same key. To enable OSPF area authentication, execute the area authentication command in routing process configuration mode. The authentication can be enabled separately on an interface by executing the ip ospf authentication command in interface configuration mode. When both the interface and the area are configured with authentication, the one for the interface takes precedence. The FSOS software supports smooth modification of MD5 authentication keys, which shall be added before deleted. When an MD5 authentication key of the device is added, the device will regard other devices have not had new keys and thus send multiple OSPF packets by using different keys, till it confirms that the neighbors have been configured with new keys. When all devices have been configured with new keys, it is possible to delete the old key.	
Configuration Examples	The following example adds a new OSPF authentication key "hello5" with key ID 5 for fastEthernet 0/1. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0 FS(config-if-FastEthernet 0/1)# ip ospf authentication message-digest FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10 FS(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5md5 hello5</pre> When all neighbors are added with new keys, the old keys shall be deleted for all devices. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# no ip ospf message-digest-key 10md5 hello10</pre>	

Related Commands	Command	Description
	area authentication	Enables OSPF area authentication and defines authentication mode.
	ip ospf authentication	Enables authentication on the interface and defines authentication mode.
Platform Description	N/A	

2.36 ip ospf mtu-ignore

	Use this command to disable the MTU check when an interface receives the database description packet. Use the no form of this command to restore the default setting.	
	ip ospf mtu-ignore	
	no ip ospf mtu-ignore	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	MTU check is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	After receiving the database description packet, the device will check whether the MTU of the neighbor interface is the same as its own MTU. If the received database description packet indicates an MTU greater than the interface's MTU, the neighboring relationship cannot be established. This can be fixed by disabling the MTU check.	
Configuration Examples	The following example disables the MTU check function on fastEthernet 0/1. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip ospf mtu-ignore</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.37 ip ospf network

	Use this command to configure the OSPF network type in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf network { broadcast non-broadcast 	
	point-to-multipoint [non-broadcast] point-to-point }	
	no ip ospf network	
Parameter Description	Parameter	Description
	broadcast	Sets the OSPF network type as the broadcast type.
	non-broadcast	Sets the OSPF network type as the non-broadcast multi-path access type, i.e. NBMA network.
	point-to-multipoint [non-broadcast]	Sets the OSPF network type as the point-to-multipoint type. The value is the point-to-multipoint broadcast type by default. The non-broadcast option means the point-to-multipoint non-broadcast type.
	point-to-point	Sets the OSPF network type as the point-to-point type.
Defaults	The default configurations are as follows: PTP network type: Point-to-Point Protocol(PPP), Serial Line Internet Protocol(SLIP), frame relay point-to-point (PTP) sub-interface, X.25 PTP sub-interface encapsulation NBMA network type: frame relay (except for PTP sub-interface), X.25 encapsulation (except for PTP sub-interface) Broadcast network type: Ethernet encapsulation By default, the network type is the point-to-multipoint network type.	
Command Mode	Interface configuration mode	
Usage Guide	The broadcast type requires that the interface must have the broadcast capability. The P2P type requires that the interfaces are interconnected in one-to-one manner. The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other. The P2MP type does not raise any requirement.	
Configuration Examples	The following example configures the frame relay interface network as the P2P type. <pre>FS(config)# interface Serial 1/0 FS(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0 FS(config-Serial 1/0)# encapsulation frame-relay FS(config-Serial 1/0)# ip ospf network point-to-point</pre> The following example configures the frame relay interface network as the NBMA type. <pre>FS(config)# interface Serial 1/0 FS(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0 FS(config-Serial 1/0)# encapsulation frame-relay FS(config-Serial 1/0)# ip ospf network non-broadcast</pre>	

	<pre>FS(config-Serial 1/0)#exit FS(config)# router ospf 20 FS(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150</pre>	
Related Commands	Command	Description
	dialer map ip	Defines the mapping between IP address and dialing number.
	frame-relay map	Defines the mapping between IP address and frame DLCI.
	neighbor(OSPF)	Defines the IP address of neighbor applicable to NBMA network type and point-to-multipoint non-broadcast type only.
	X25 map	Defines the mapping between IP address and X.25 network address.
Platform Description	N/A	

2.38 ip ospf priority

	Use this command to configure the OSPF priority in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf priority <i>priority</i>	
	no ip ospf priority	
Parameter Description	Parameter	Description
	<i>priority</i>	Sets the OSPF priority of the interface in the range from 0 to 255.
Defaults	The default is 1.	
Command Mode	Interface configuration mode	
Usage Guide	The interface priority is included in the Hello packet. When DR/BDR election occurs in the OSPF broadcast type network, the device with higher priority will become the DR or BDR. If the devices have the same priority, the one with higher ID will become the DR or BDR. The device with priority 0 cannot become DR or BDR. This command is valid only for OSPF broadcast and non-broadcast network types.	
Configuration Examples	The following example configures the priority of fastethernet 0/1 as 0. <pre>Switch(config)#interface fastethernet 0/1 FS(config-if-FastEthernet 0/1)# ipospfpriority0</pre>	

Related Commands	Command	Description
	ip ospf network	Configures the network type of the interface.
Platform Description	N/A	

2.39 ip ospf retransmit-interval

	Use this command to define the interval for sending the link state update (LSU) packet on the interface in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf retransmit-interval <i>seconds</i>	
	ip ospf retransmit-interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for sending the LSU packets in seconds. The range is from 1 to 65535. This interval must be greater than the round trip delay of packets between two neighbors.
Defaults	The default is 5.	
Command Mode	Interface configuration mode	
Usage Guide	After the device sends an LSU packet, the LSU packet stays in the transmission buffer queue. If no confirmation from the neighbor is obtained in the interval defined with the ip ospf retransmit-interval command, the LSU will be sent once again. In serial lines or virtual links, the retransmission interval shall be slightly larger. The LSU packet retransmission interval of virtual links is defined with the area virtual-link command followed with the keyword retransmit-interval.	
Configuration Examples	The following example configures the LSU packet retransmission interval on fastEthernet 0/1 as 10 seconds. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10</pre>	
Related Commands	Command	Description
	area virtual-link	Defines an OSPF virtual link.
Platform Description	N/A	

2.40 ip ospf source-check-ignore

	Use this command to disable the source address check in the point-to-point link. Use the no form of this command to restore the default setting	
	ip ospf source-check-ignore	
	no ip ospf source-check-ignore	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	For OSPF, the source address of the received packet is required to be in the same network segment with the receiving interface. However, in a point-to-point link, the addresses of two ends of the link are individually set, and they are not required to be in the same network segment. The peer address is informed during the process of point-to-point link negotiation; therefore, OSPF will check whether the source address of the packet is the informed one. If no, the OSPF regards this packet as illegal and drops it. In some applications, the addresses informed during the negotiation are shielded. You need to disable the source address check to ensure the normal establishment of OSPF neighbors. The source address check shall be never enabled, especially for the unnumbered interfaces.	
Configuration Examples	The following example disables the source address check function in the point-to-point link. <pre>FS(config)# interface serial 1/0 FS(config-if)# ip ospf source-check-ignore</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.41 ip ospf subvlan

	Use this command to enable OSPF on super VLANs. Use the no form of this command to restore the default setting.	
	ip ospf subvlan [all vid]	
	no ip ospf subvlan	

Parameter Description	Parameter	Description
	all	Indicates that packets are allowed to be sent to all sub VLANs.
	vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Defaults	The default setting takes effect only on super VLANs with OSPFv3 disabled.	
Command Mode	Interface configuration mode	
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor flap.	
Configuration Examples	The following example sends OSPF multicast packets to sub VLAN 1024 of super VLAN 300. <pre>FS(config)# interface vlan 300 FS(config-if-VLAN 300)# ip ospf subvlan 1024</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.42 ip ospf transmit-delay

	Use this command to define the LSU packet transmission delay in interface configuration mode. Use the no form of this command to restore the default setting.	
	ip ospf transmit delay <i>seconds</i>	
	no ip ospf transmit delay	
Parameter Description	Parameter	Description
	<i>seconds</i>	LSU packet transmission delay in seconds in the range from 1 to 65535.
Defaults	The default is 1.	

Command		
Mode	Interface configuration mode	
Usage Guide	Before the LSU packet is transmitted, the Age field in all the LSAs of the packet will be increased by the value defined with the ip ospf transmit-delay command in interface configuration mode. The configuration of this parameter shall consider the transmission and line transmission delay of the interface. For low-rate lines, the transmission delay of the interface shall be slightly larger. The LSU packet transmission delay of the virtual link is defined with the area virtual-link command followed with the keyword retransmit-interval. The FSOS software will resend or request resending the LSA with Age up to 3600. If no update is obtained in time, the aged LSA will be cleared from the link state database.	
Configuration	The following example configures the transmission delay of fastEthernet 0/1 as 10.	
Examples	<pre>FS(config)# interface fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10</pre>	
Related		
Commands	Command	Description
	area virtual-link	Defines an OSPF virtual link.
Platform	N/A	
Description		

2.43 ispf enable

	Use this command to enable the ISPF function. Use the no form of this command to disable the ISPF function.	
	ispf enable	
	no ispf enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	ISPF is disabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	OSPF adopts the SPF algorithm to calculate the network topology within an area. SPF algorithm is run for each area independently, Incremental SPF algorithm (ISPF) is an area-based algorithm, If the topology changes, the ISPF algorithm will calculate only the affected notes of the topology rather than calculating the entire tree, which speeds up the OSPF route convergence and saves CPU resources. Because the ISPF algorithm is not shared among routers, each router within the same network can have a unique	

	ISPF algorithm. To ensure a faster OSPF convergence, the ISPF function should be enabled on every router within the network. Enabling ISPF function only affects the choice of topology calculating algorithm for OSPF. So you can configure the delay time for the ISPF with the timers spf command and the timers throttle spf command as well.	
Configuration Examples	The following example enables the ISPF function. <pre>FS(config)# router ospf 1 FS(config-router)# ispf enable</pre> The following example enables the ISPF function on the specified VRF. <pre>FS(config)# router ospf 1 vrf vpn1 FS(config-router)# ispf enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.44 log-adj-changes

	Use this command to enable the logging of the neighbor state changes. Use the no form of the command to disable this function.	
	log-adj-changes [detail]	
	no log-adj-changes [detail]	
Parameter Description	Parameter	Description
	detail	Records the detail of changes.
Defaults	This function is enabled by default. Without the detail parameter, the system records the logs that the neighbor enters or exits the full state.	
Command Mode	Routing process configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example logs the neighbor state changes. <pre>FS(config)# router ospf 1 FS(config-router)# log-adj-changes detail</pre>	

Related Commands	Command	Description
	show ip ospf	Displays the OSPF global configuration information.
Platform Description	N/A	

2.45 max-concurrent-dd

	Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the no form of this command to restore the default setting.	
	max-concurrent-dd <i>number</i>	
	no max-concurrent-dd	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of DD packets in the range from 1 to 65535
Defaults	The default is 5.	
Command Mode	Routing process configuration mode	
Usage Guide	When a router is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have at the same time.	
Configuration Examples	The following example sets the maximum number of DD packets to 4. After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors. <pre>FS(config)# routerospf10 FS(config-router)# max-concurrent-dd4</pre>	
Related Commands	Command	Description
	router ospf max-concurrent-dd	Sets the maximum number of neighbors allowed in concurrent interaction for all OSPF routing processes.
Platform Description	N/A	

2.46 max-metric

	Use this command to set the maximum metric of the router-lsa, so that this routing device will not firstly be used as the transmission node by other devices in SPF computing. Use the no form of this command to restore the default setting.

	max-metric router-lsa [external-lsa [<i>max-metric-value</i>]] [include-stub] [on-startup [<i>seconds</i>]] [summary-lsa [<i>max-metric-value</i>]]	
	no max-metric router-lsa [external-lsa [<i>max-metric-value</i>]] [include-stub] [on-startup [<i>seconds</i>]] [summary-lsa [<i>max-metric-value</i>]]	
Parameter Description	Parameter	Description
	router-lsa	Configures the maximum metric (0XFFFF) of non-stub links in the Router LSA.
	external-lsa	Uses the maximum metric instead of the external-lsa metric (including the Type-5 and Type-7).
	<i>max-metric-value</i>	Maximum metric of the LAS. The range is 1 to 16777215. The default value is 16711680.
	include-stub	Configures the maximum metric of the stub links in the Router LSA.
	on-startup	Advertises the maximum metric when the routing device starts up.
	<i>seconds</i>	Interval of advertising the maximum metric. The range is 5 to 86400. The default value is 600 seconds.
	summary-lsa	Uses the maximum metric to replace the summary LSA metric. (including Type-3 and Type-4)
Defaults	The normal metric LSAs are used by default.	
Command Mode	Routing process configuration mode	
Usage Guide	With the max-metric router-lsa command enabled, the maximum metric of non-stub links in the Router LSA generated by the routing device is set. The link's normal metric is restored after canceling this configuration or reaching the timer. By default, with this command enabled, the normal metric of the stub links is still advertised, which is the output interface cost. If the include-stub parameter is configured, the maximum metric of the stub links will be advertised. When the device acts as an ABR, if no interval flow transmission is expected, use the summary-lsa parameter to set the summary LSA as the maximum metric. When the device acts as an ASBR device, if no external flow transmission is expected, use the external lsa parameter to set the external LSA as the maximum metric. The max-metric router-lsa command is usually used in the following scenes: The device is restarted, which generally makes the IGP protocol converge faster, so that other devices attempt forwarding the dataflow through the new started-up device. If the current device remains establishing a BGP routing table, the packets sent to these networks will be discarded due to some BGP routings have not been learned. In this case, use the on-startup parameter to set certain delay, so that this device can serve as a transmission node after restarting. The device is added into the network without being used for dataflow transmission. If the backup path exists, the current device is not used for the dataflow transmission. Otherwise, this device is still used to transmit the dataflow. Remove the device from the network gracefully. With this command enabled, the current device advertises the	

	maximum metric to all devices, as that the other devices in this network can choose the backup path to for the dataflow transmission before the current device is removed.  For the OSPF implementation in the earlier versions (RFC 1247 or earlier versions), the links with the maximum metric (0xFFFF) in the LSA will not participate in the SPF calculation, that is, no dataflow will be sent to the router that have generated these LSAs.	
Configuration Examples	The following example configures the LSA maximum metric as 100 seconds after starting the device. <pre>FS(config)# router ospf 20 FS(config-router)# max-metric router-lsa on-startup 100</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF related configurations.
Platform Description	N/A	

2.47 neighbor

	Use this command to define the OSPF neighbor in routing process configuration mode. Use the no form of this command to restore the default setting.	
	Neighbor <i>ip-address</i> [poll-interval <i>seconds</i>] [priority <i>priority</i>] [cost <i>cost</i>]	
	no neighbor <i>ip-address</i> [[poll-interval] [priority]] [<i>cost</i>]	
Parameter Description	Parameter	Description
	<i>ip address</i>	IP address of the neighbor
	poll-interval <i>seconds</i>	(Optional) Specifies the interval of polling neighbors in seconds. The range is from 0 to 2147483647. Only the non-broadcast (NBMA) network type supports this option.
	priority <i>priority</i>	(Optional) Configures the priority of non-broadcast network neighbors. The range is from 0 to 255. Only the non-broadcast (NBMA) network type supports this option.
	cost <i>cost</i>	(Optional) Configures the cost to each neighbor in point-to-multipoint network, not defined by default, where the cost configured on the interface will be used. The range is from 0 to 65535. Only the point-to-multipoint [non-broadcast] network type supports this option.
Defaults	No neighbor is defined by default. The default neighbor polling interval is 120 seconds. The default NBMA neighbor priority is 0.	

Command Mode	Routing process configuration mode	
Usage Guide	The FSOS software must explicitly configure the neighbor information for every non-broadcast network neighbor. The IP address of a neighbor must be the master IP address of that neighbor interface. In the NBMA network, if the neighbor device becomes inactive, in other words, if the Hello packet is not received within the device dead-interval, the OSPF will send more Hello packets to the neighbor. The interval at which the Hello packets are sent is called the polling interval. When the OSPF starts to work for the first time, it sends Hello packets only to the neighbor whose priority is not 0, so that the neighbor whose priority is set as 0 will not participate in the DR/BDR election. When the DR/BDR is generated, the DR/BDR sends the Hello packets to all neighbors to establish the neighbor relationship. Since the point-to-multipoint non-broadcast network has no broadcast capability, neighbors cannot be found dynamically. So, it is required to use this command to manually configure neighbor. In addition, it is possible to configure the cost to each neighbor through the cost option for the point-to-multipoint network type.	
Configuration Examples	The following example declares an OSPF non-broadcast network neighbor, with the IP address 172.16.24.2, priority 1 and polling interval 150 seconds. <pre>FS(config)# routerospf 20 FS(config-router)# network 172.16.24.0 0.0.0.255 area 0 FS(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150</pre>	
Related Commands	Command	Description
	ip ospf priority	Sets the interface priority.
	ip ospf network	Sets the network type
Platform Description	N/A	

2.48 nsr

	Use this command to enable the nonstop routing (NSR) function for the OSPF instance. Use the no form of this command to disable the NSR function.	
	nsr	
	no nsr	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	NSR is disabled by default.	
Command Mode	Routing process configuration mode	

Usage Guide	NSR enables the device to recover link state and regenerate routes without the assistance from neighbors during active/standby switchover of distributed devices or stacking system. The backup information includes adjacencies and OSPF state. You need to enable either NSR or GR in the same OSPF process. That is, the NSR feature will be disabled after the GR feature is enabled. Similarly, the GR feature will be disabled after NSR is enabled, and the GR Helper capability is still supported. The active/standby switchover of distributed devices or stacking system takes a period of time. If the OSPF dead interval is less than the switchover period, OSPF neighbors will be disconnected and the services will be interrupted. It is recommended to configure the OSPF dead interval longer than its default value. It is not recommended to enable the Fast Hello feature after NSR is enabled, because OSPF dead interval is less than 1 second when the Fast Hello feature is enabled and the OSPF neighbors are disconnected and NSR becomes ineffective.	
Configuration Examples	The following example enables NSR. <pre>FS(config)#router ospf 1 FS(config-router)# nsr</pre>	
Related Commands	Command	Description
	router ospf	Creates the OSPF routing process.
Platform Description	N/A	

2.49 network area

	Use this command to define which interfaces run OSPF and the OSPF areas they belong to in routing process configuration mode. Use the no form of this command to restore the default setting.	
	network <i>ip-address wildcard area area-id</i>	
	no network <i>ip-address wildcard area area-id</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IP address of the interface
	<i>wildcard</i>	Defines the comparison bits in the IP address, with 0 for exact match and 1 for no comparison
	<i>area-id</i>	OSPF area identifier. An OSPF area is always associated with an address range. For easy of management, a subnet can be used as the OSPF area identifier.
Defaults	No OSPF area is configured by default.	
Command Mode	Routing process configuration mode	

Usage Guide	The ip-address and wildcard parameters allow associating multiple interfaces with one OSPF area. To run OSPF on an interface, it is required to include the primary IP address and secondary IP address of the interface in the IP address range defined by the network area command. If only the secondary IP address is included, OSPF cannot be enabled on the interface. You can determine the OSPF process that the interface takes part in by the means of the best match if the IP address of the interface matches the IP address ranges defined by the network command in multiple OSPF processes.	
Configuration Examples	The following example defines: Three areas: 0, 1 and 172.16.16.0 The interfaces whose IP addresses fall into the 192.168.12.0/24 range to area 1 The interfaces whose IP addresses fall into the 172.16.16.0/20 range to area 2 The remaining interface being assigned to area 0. <pre>FS(config)# routerospf 20 FS(config-router)# network172.16.16.0 0.0.15.255 area172.16.16.0 FS(config-router)# network192.168.12.0 0.0.0.255 area 1 FS(config-router)# network0.0.0.0 255.255.255.255 area0</pre>	
Related Commands	Command	Description
	router ospf	Creates the OSPF routing process.
Platform Description	N/A	

2.50 overflow database

	Use this command to configure the maximum number of LSAs supported by the current OSPF instance. Use the no form of this command to restore the default setting.	
	overflow database <i>number</i> [hard soft]	
	no overflow database	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of LSAs. The range is from 1 to 4294967294.
	hard soft	hard: shuts down the OSPF instance when the number of LSAs exceeds that number. soft: issues an alarm when the number of LSAs exceeds that number.
Defaults	The maximum number of LSAs supported by the current OSPF instance is not restricted by default.	

Command Mode	Routing process configuration mode	
Usage Guide	To shut down the OSPF instance when the number of LSAs exceeds that number, use the hard parameter; otherwise, use the soft parameter.	
Configuration Examples	The following example configures that OSPF instance 10 will be shut down when there are more than 10 LSAs. <pre>FS(config)# router ospf 10 FS(config-router)# overflow database 10 hard</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.51 overflow database external

	Use this command to configure the maximum number of external LSAs and the waiting time from the overflow state to the normal state. Use the no form of this command to restore the default setting.	
	overflow database external <i>max-dbsize wait-time</i>	
	no overflow database external	
Parameter Description	Parameter	Description
	<i>max-dbsize</i>	Maximum number of external LSAs (the value shall be the same for all routing devices in the same AS). The range is from 0 to 2147483647.
	<i>wait-time</i>	Waiting time of the routing device from the overflow status to normal status. The range is from 0 to 2147483647.
Defaults	The maximum number of external-LSAs is not restricted by default. If the maximum number of external-LSAs is restricted, the normal status cannot be restored when the maximum number is exceeded.	
Command Mode	Routing process configuration mode	
Usage Guide	When the number of external-LSAs exceeds the value of max-db size, the device enters the overflow state. Then no more external-LSA will be loaded and the external-LSAs generated locally will be cleared. After wait-time expires, the device restores to the normal state and external-LSAs are reloaded.  When using this function, ensure that all routers of the OSPF backbone area and common areas use the same max-db size value. Otherwise, the following situations occur:	

	 The link status is inconsistent on the entire network and neighbors fail to achieve the Full state.  Incorrect routes occur, including loops.  AS-External-LSAs may be frequently retransmitted.	
Configuration Examples	The following example configures that the maximum number of external LSAs is 10, and it turns to the overflow status upon timeout, and the time interval attempting to restore from the overflow state to the normal state is 3 seconds. <pre>FS(config)# routerospf10 FS(config-router)# overflow database external10 3</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.52 overflow memory-lack

	Use this command to allow OSPF to enter the OVERFLOW state when the memory lacks. Use the no form of this command to disable this function.	
	overflow memory-lack	
	no overflow memory-lack	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default	
Command Mode	Routing process configuration mode	
Usage Guide	The action of OSPF entering the OVERFLOW state is to discard the newly-learned external route and effectively prevent the memory from increasing. It is possible that enabling this function causes the route loop in the whole network. To reduce that possibility, OSPF will generate a default route directing to the NULL port and this default route will exist in the OVERFLOW state. Use the clear ip ospf process command to reset the OSPF and remove the OSPF OVERFLOW state. Use the no form of this command to prevent the OSPF to enter the OVERFLOW state when the memory is insufficient, which may result in the constantly consumption of the memory resources. If the memory is exhausted to some degree, the OSPF instance will stop and all learned routes will be removed.	

Configuration Examples	The following example prevents the OSPF from entering the OVERFLOW state when the memory is insufficient.	
	<pre>FS(config)# router ospf 1 FS(config-router)# no overflow memory-lack</pre>	
Related Commands	Command	Description
	clear ip ospf process	Resets the OSPF instances.
	show ip protocols ospf	Displays the OSPF information.
Platform Description	N/A	

2.53 passive-interface

	Use this command to configure the specified network interface or all interface as the passive interfaces. Use the no form of this command to restore the default setting.	
	passive-interface { default <i>interface-type interface-number</i> <i>interface-type interface-number ip-address</i> }	
	no passive-interface { default <i>interface-type interface-number</i> <i>interface-type interface-number ip-address</i> }	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Interface to be set as a passive interface
	default	Sets all the interfaces as passive interfaces
	<i>interface-type interface-number ip-address</i>	Sets the address of the specified interface as a passive address.
Defaults	No interface is configured as a passive interface by default. All interfaces are allowed to receive or send OSPF packets.	
Command Mode	Routing process configuration mode	
Usage Guide	To prevent other devices in the network from dynamically learning the routing information of the device, set the specified network interface of this device as a passive interface or the IP address of the specified network interface as a passive address	
Configuration Examples	The following example configures fastEthernet 0/1 as a passive interface and the IP address of the interface 1.1.1.1 as the passive address.	
	<pre>FS(config)# routerospf 30 FS(config-router)# passive-interface fastEthernet 0/1 FS(config-router)# passive-interface fastEthernet 0/1 1.1.1.1</pre>	
Related Commands	Command	Description

	show ip ospf interface	Displays the configuration information of the interface.
Platform	N/A	
Description		

2.54 redistribute

	Use this command to redistribute the external routing information. Use the no form of this command to restore the default setting.	
	redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static } [{ level-1 level-1-2 level-2 }] [match { internal external [1 2] nssa-external [1 2] }] [metric <i>metric-value</i>] [metric-type { 1 2 }] [route-map <i>route-map-name</i>] [subnets] [tag <i>tag-value</i>]	
	no redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static } [{ level-1 level-1-2 level-2 }] [match { internal external [1 2] nssa-external [1 2] }] [metric <i>metric-value</i>] [metric-type { 1 2 }] [route-map <i>route-map-name</i>] [subnets] [tag <i>tag-value</i>]	
Parameter Description	Parameter	Description
	bgp	Redistribution from bgp
	connected	Redistribution from direct routes
	isis [<i>area-tag</i>]	Redistribution from an IS-IS instance specified in <i>area-tag</i>
	ospf <i>process-id</i>	Redistribution from an ospf instance specified in <i>process-id</i> in the range from 1 to 65,535
	rip	Redistribution from rip
	static	Redistribution from static routes
	level-1 level-1-2 level-2	Configures IS-IS route redistribution. The parameter specifies a level, and routes of this level will be redistributed. Only level-2 IS-IS routes can be redistributed by default.
	match	Filters specified routes for configuring OSPF route redistribution. By default, all the OSPF routes are redistributed.
	metric <i>metric-value</i>	Specifies the metric of an OSPF external LSA in the range from 0 to 16777214.
	metric-type {1 2}	Sets the external routing type as E-1 or E-2.
	route-map <i>route-map-name</i>	Redistribution filter rule
	subnets	Redistributes the routes of non standard networks.
	tag <i>tag-value</i>	Sets the tag value of the routes redistributed to the OSPF in the range from 0 to 4294967295.
Defaults	Redistribution configuration is not supported by default. If you configure OSPF redistribution, all subtype routes of the instance are redistributed. If you configure ISIS redistribution, all level-2 subtype routes of the instance are redistributed. In other cases, all routings of this type are redistributed. The default metric of the redistribution BGP route is 1. The default metric of LSAs generated by routes of other types is 20.	

	The default value of metric-type is E-2. No route-map is associated by default.
Command Mode	Route configuration mode
Usage Guide	After the command is configured, the router will become an ASBR, and the related routing information is imported into the OSPF domain and broadcasted to other OSPF routers through type-5 LSAs. When you configure is route redistribution without the level parameter, level-2 routes can be redistributed by default. In initial redistribution configuration that carries the level parameter, routes of the specified level can be redistributed. When you save the configuration containing both level 1 and level 2, they are merged into level-1-2 for convenience. For details, see the configuration examples. When you configure OSPF router distribution without the match parameter, the OSPF routes of all sub types are redistributed by default. Then the first configured match parameter is used as the original one. Only the routes matching the specific type can be redistributed. Use the no form of this command to restore the default configuration. When you filter routes for redistribution by following the route-map rule, the match rule of the route-map rule is specific for the original redistribution parameters. The route-map rule works only when the redistributed OSPF routes follow the match rule.  The range of set metric is from 0 to 16777214 for the associated route-map. If the value exceeds the range, introducing a route fails.  The following are the rules for configuring the no form of the redistribute command:1. If the no form specifies some parameters, restore their default values.2. If the no form contains no parameter, delete the whole command. If the following configuration exists: redistribute isis 112 level-2 You can use the no redistribute isis 112 level-2command to modify the configuration. According to preceding rules, this command restores the level-2 parameter to the default value, namely level-2. Therefore, the configuration remains the same after the no form of the preceding command is executed. redistribute isis 112 level-2 To delete the whole command, use the following command: no redistribute isis 112
Configuration Examples	The following example redistributes routes of ospf2 and isis isis-001 to the OSPF area. <pre>FS(config)# router ospf1 FS(config-router)# redistribute ospf 2 subnets FS(config-router)# redistribute ospf2match external 1 internal FS(config-router)# redistribute isisis-001 FS(config-router)# redistribute isisis-001 level-1</pre> The following example displays the output of the show run command. <pre>router ospf 1 redistribute ospf 2 match external 1 internal subnets redistribute isis isis-001 level-1-2</pre>

Related Commands	Command	Description
	summary-address	Configures the aggregate route for the external route of the OSPF route area.
	default-metric	Sets the default metric of the OSPF redistribution route.
Platform Description	N/A	

2.55 router ospf

	Use this command to create the OSPF routing process in global configuration mode. Use the no form of this command to restore the default setting.	
	router ospf	
	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	
	no router ospf <i>process-id</i>	
Parameter Description	Parameter	Description
	<i>process-id</i>	ID of an OSPF process. If the process ID is not configured, process 1 is configured.
	<i>vrf-name</i>	VRF of the configured OSPF process for products that support the VRF.
Defaults	No OSPF routing process exists by default.	
Command Mode	Global configuration mode	
Usage Guide	Based on the original implementation, the FSOS10.1 adds the routing process ID to multi-instance OSPF. Different OSPF instances are mutually independent and can be approximately considered as two routing protocols that run independently.	
Configuration Examples	The following example creates the OSPF routing process 10 within the specified vrf: vpn_1. FS(config)# router ospf10 vrf: vpn_1	
Related Commands	Command	Description
	show ip protocols	Displays the routing protocol information.
	show ip ospf	Displays the OSPF information.
Platform Description	N/A	

2.56 router ospf max-concurrent-dd

	Use this command to specify the maximum number of DD packets that can be processed (initiated or accepted) at the same time. Use the no form of this command to restore the default setting.	
	router ospf max-concurrent-dd <i>number</i>	
	no router ospf max-concurrent-dd	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of DD packets in the range from 1 to 65535.
Defaults	The default is 10.	
Command Mode	Global configuration mode	
Usage Guide	When a routing device is exchanging data with multiple neighbors, its performance will be affected. This command is configured to limit the maximum number of DD packets that each OSPF instance can have (initiated or accepted) at the same time.	
Configuration Examples	The following example sets the maximum number of DD packets to 4. After the configuration, the device can initiate to interact with four neighbors and can concurrently accept the interaction. That is, the device can interact with a maximum of eight neighbors. <pre>FS# configure terminal FS(config)# router ospfmax-concurrent-dd4</pre>	
Related Commands	Command	Description
	max-concurrent-dd	Sets the maximum number of the neighbors that the OSPF routing process can concurrently interact with.
Platform Description	N/A	

2.57 router-id

	Use this command to set the router ID. Use the no form of this command to restore the default setting.	
	router-id <i>router-id</i>	
	no router-id	
Parameter Description	Parameter	Description
	<i>router-id</i>	Router ID in IP address form

Defaults	The OSPF routing process will select the maximal interface IP address as the router ID by default. If the loopback interface of an IP address is not configured, the OSPF routing process will select the maximum IP address among all its physical interfaces as the router ID.	
Command Mode	Routing process configuration mode	
Usage Guide	You can configure any IP address as the router ID. However, the router ID should be unique. Note that once the router ID changes, the OSPF protocol will do a lot of processing. Therefore, it is not recommended to change the router ID. The device can be changed only when no LSA is generated.	
Configuration Examples	The following example modifies the router ID to 0.0.0.36. <pre>FS(config)# router ospf 20 FS(config-router)# router-id 0.0.0.36</pre>	
Related Commands	Command	Description
	show ip protocols	Displays the routing protocol information.
Platform Description	N/A	

2.58 show ip ospf

	Use this command to display the OSPF information.	
	show ip ospf [<i>process-id</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command displays the information of the OSPF routing process.	
Configuration Examples	The following example displays the output of the show ip ospf command. <pre>FS# show ip ospf Routing Process "ospf 1" with ID 1.1.1.1 Domain ID type 0x0105, value 0x010101010101 Process uptime is 4 minutes Process bound to VRF default</pre>	

```

Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag is enabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
Condition:on startup for 100 seconds, State:inactive
Advertise stub links with maximum metric in router-LSAs
Advertise summary-LSAs with metric 16711680
Advertise external-LSAs with metric 16711680
Unset reason:timer expired, Originated for 100 seconds
Unset time:00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group:240 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjacency Changes :Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
BFD enabled
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
Number of LSA 3. Checksum 0x0204bf
Area 1 (NSSA)
Number of interfaces in this area is 1(1)

```

Number of fully adjacent neighbors in this area is 0
 Number of fully adjacent virtual neighbors through this area is 0
 Area has no authentication
 SPF algorithm last executed 02:09:23.040 ago
 SPF algorithm executed 4 times
 Number of LSA 6. Checksum 0x028638
 NSSA Translator State is disabled, Stability Interval expired in 00:00:03

Field	Description
Router ID	ID of a router.
Process uptime	Effective time of the current OSPF process (the process does not take effect when device-id is 0.0.0.0)
Bou to VRF	VRF of the current OSPF
Conforms to RFC2328	Same as the RFC2328
RFC1583Compatibilit flag	Whether the RFC1583 or RFC2328 is adopted for the calculation of external routes. This policy is used in the selection of best ASBR and in the route comparison.
Support Tos	Supports Only TOS0.
Supports opaque LSA	Supports opaque-LSA.
Graceful-restart	GR Restart capability described in the RFC3623 Graceful Restart
Graceful-restart helper	GR Help capability described in the RFC3623 Graceful Restart
Router Type	OSPF device type, including normal, ABR, and ASBR
SPF Delay	Delay before the SPF calculation is invoked after the topology change is received
SPF-holdtime	Minimum holdtime between two SPF calculations
LsaGroupPacing	Parameter used for LSA pacing, checksum calculation, and aging interval
Incomming current DD exchange neighbors	Number of neighbors under interaction. The incoming neighbors are those entering the exstart status for the first time.
Outgoing current DD exchange neighbors	Number of neighbors under interaction. The outgoing neighbors are those exiting from the higher status to the exstart status for re-interaction.

Number of external LSA	Number of external LSAs stored in the database
External LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of opaque LSA	Number of external LSAs stored in the database
Opaque LSA Checksum Sum	Checksum sum of external LSAs stored in the database
Number of non-default external LSA	Number of external LSAs with non-default routes
External LSA database limit	Limit of external LSA number
Exit database overflow state interval	Time of exiting the overflow status
Database overflow state	Whether the current OSPF process is in the overflow status
Number of LSA originated	Number of LSAs generated
Number of LSA received	Number of LSAs received
Log Neighbor Adjency Changes	Whether the record switch for neighbor status change is enabled
Number of areas attached to this router	Total number of areas on the devices
Area type	Area type, including normal, stub, and nssa
Number of interfaces in this area	Number of interfaces in this area
Number of fully adjacent neighbors in this area	Number of Full neighbors of the area
Number of fully adjacent virtual neighbors through this area	Number of Full neighbors with virtual connections in the area. It is effective only in the non-backbone default-type areas.
Area authentication	Authentication mode of the area
SPF algorithm last executed	Time from the previous SPF calculation to the current time
SPF algorithm executed times	Times of SPF calculations
Number of LSA	Total number of LSAs in this area
Checksum Sum	Checksum sum of the LSAs in the area

	NSSATranslatorState	Whether to convert the NSSA LSA to External LSA. It is effective on the ABR OSPF process in the NSSA.
	BFD enabled	Enables BFD for OSPF.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.59 show ip ospf border-routers

	Use this command to display the OSPF internal routing table on the ABR/ASBR.											
	show ip ospf [process-id] border-routers											
Parameter Description	Parameter	Description										
	process-id	OSPF process ID										
Defaults	N/A											
Command Mode	Privileged EXEC mode											
Usage Guide	This command displays the OSPF internal routes from the local routing device to the ABR or ASBR. The OSPF internal routing table is different from the one displayed with the show ip route command. The OSPF internal routing table has the destination address of the router ID instead of the destination network.											
Configuration Examples	The following example displays the output of the show ip ospf border-mrouters command. FS# show ip ospf border-routers OSPF internal Routing Table Codes:i - Intra-area route, I - Inter-area route i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select The following table describes fields in the output. <table><tr><th>Field</th><th>Description</th></tr><tr><td>Codes</td><td>Route type code, where “i” means intra-area routes, while “I” means inter-area routes.</td></tr><tr><td>I</td><td>Intra-area routes</td></tr><tr><td>1.1.1.1</td><td>Displays the OSPF ID of the border device.</td></tr><tr><td>[2]</td><td>Displays the cost to the border device.</td></tr></table>		Field	Description	Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.	I	Intra-area routes	1.1.1.1	Displays the OSPF ID of the border device.	[2]	Displays the cost to the border device.
Field	Description											
Codes	Route type code, where “i” means intra-area routes, while “I” means inter-area routes.											
I	Intra-area routes											
1.1.1.1	Displays the OSPF ID of the border device.											
[2]	Displays the cost to the border device.											

	via 10.0.0.1	Displays the next-hop gateway to the border device.
	FastEthernet 0/1	Displays the interface to the border device.
	ABR, ASBR	Displays the type of the border device, including ABR, ASBR, or both.
	Area 0.0.0.1	Displays the area that learns the route.
	select	Indicates the currently selected optimal path when there are multiple paths to the ASBR.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.60 show ip ospf database

	Use this command to display the OSPF link state database information. Use the no form of this command to restore the default setting. Different formats of the command will display different LSA information.	
	show ip ospf [<i>process-id</i> [<i>area-id</i> <i>ip-address</i>]] database [{ asbr-summary external network nssa-external opaque-area opaque-as opaque-link router summary }] [{ adv-router <i>ip-address</i> self-originate } <i>link-state-id</i> brief] [database-summary max-age detail]	
Parameter Description	Parameter	Description
	area-id	(Optional) Displays the area ID.
	adv-device	(Optional) Displays the LSA information generated by the specified advertising device.
	link-state-id	(Optional) Displays the LSA information of the specified OSPF link state identifier.
	self-originate	(Optional) Displays the LSA information generated by the device itself.
	Max-age	(Optional) Displays the LSAs aged.
	router	(Optional) Displays the OSPF device LSA information.
	network	(Optional) Displays the OSPF network LSA information.
	summary	(Optional) Displays the OSPF summary LSA information.
	asbr-summary	(Optional) Displays the ASBR summary LSA information.
	external	(Optional) Displays the OSPF external LSA information.
	nssa-external	(Optional) Displays the category 7 OSPF external LSA information.
	opaque-area	(Optional) Displays type 10 LSAs.
	opaque-as	(Optional) Displays type 11 LSAs.
	opaque-link	(Optional) Displays type 9 LSAs.
	database-summary	(Optional) Displays the statistics of LSAs of the link state database.
	detail	Displays detailed information of LSAs of the OSPF.
	brief	Displays the brief information of the LSAs of the specified type.

Defaults	N/A										
Command Mode	Privileged EXEC mode										
Usage Guide	When the OSPF link state database is very large, you should display the information on the link state database by item. Proper use of commands may help OSPF troubleshooting.										
Configuration Examples	The following example displays the output of the show ip ospf database command. <pre> FS# show ip ospf database OSPF Device with ID (1.1.1.1) (Process ID 1) Device Link States (Area 0.0.0.0) Link ID ADV Device Age Seq# CkSum Link count 1.1.1.1 1.1.1.1 2 0x80000011 0x6f39 2 3.3.3.3 3.3.3.3 120 0x80000002 0x26ac 1 Network Link States (Area 0.0.0.0) Link ID ADV Device Age Seq# CkSum 192.88.88.27 1.1.1.1 120 0x80000001 0x5366 Summary Link States (Area 0.0.0.0) Link ID ADV Device Age Seq# CkSum Route 10.0.0.0 1.1.1.1 2 0x80000003 0x350d 10.0.0.0/24 100.0.0.0 1.1.1.1 2 0x8000000c 0x1ecb 100.0.0.0/16 Device Link States (Area 0.0.0.1 [NSSA]) Link ID ADV Device Age Seq# CkSum Link count 1.1.1.1 1.1.1.1 2 0x80000001 0x91a2 1 Summary Link States (Area 0.0.0.1 [NSSA]) Link ID ADV Device Age Seq# CkSum Route 100.0.0.0 1.1.1.1 2 0x80000001 0x52a4 100.0.0.0/16 192.88.88.0 1.1.1.1 2 0x80000001 0xbb2d 192.88.88.0/24 NSSA-external Link States (Area 0.0.0.1 [NSSA]) Link ID ADV Device Age Seq# CkSum Route Tag 20.0.0.0 1.1.1.1 1 0x80000001 0x033c E2 20.0.0.0/24 0 100.0.0.0 1.1.1.1 1 0x80000001 0x9469 E2 100.0.0.0/28 0 AS External Link States Link ID ADV Device Age Seq# CkSum Route Tag 20.0.0.0 1.1.1.1 380 0x8000000a 0x7627 E2 20.0.0.0/24 0 100.0.0.0 1.1.1.1 620 0x8000000a 0x0854 E2 100.0.0.0/28 0 </pre> The following table describes the fields in the output of the show ip ospf database command. <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>OSPF Device with ID</td><td>Displays the Router ID.</td></tr> <tr> <td>Device Link States</td><td>Displays the device LSA information.</td></tr> <tr> <td>Net Link States</td><td>Displays the network LSA information.</td></tr> <tr> <td>Summary Net Link</td><td>Displays the summary network LSA information.</td></tr> </table>	Field	Description	OSPF Device with ID	Displays the Router ID.	Device Link States	Displays the device LSA information.	Net Link States	Displays the network LSA information.	Summary Net Link	Displays the summary network LSA information.
Field	Description										
OSPF Device with ID	Displays the Router ID.										
Device Link States	Displays the device LSA information.										
Net Link States	Displays the network LSA information.										
Summary Net Link	Displays the summary network LSA information.										

States	
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
AS External Link States	Displays the type 5 autonomous external LSA information.
Link ID	Displays the Link ID.
ADV Device	Displays the ID of the device that advertises the LSAs.
Age	Displays the keepalive period of the LSA.
Seq#	Displays the sequence number of the LSA, which is used to check aged or duplicate LSAs.
Cksum	Displays the checksum of LSAs.
Link-Count	Displays the number of links in the device LSA information.
Route	Displays the device information included in the LSA.
Tag	Displays the tag of the LSA.

The following example displays the output the **show ip ospf database asbr-summary** command.

```

FS# show ip ospf database asbr-summary
      OSPF Device with ID (1.1.1.35) (Process ID 1)
        ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|---|E|)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Device address)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
      TOS: 0   Metric: 1

```

The following table describes the fields in the output of the **show ip ospf database asbr-summary** command.

Field	Description
OSPF Device with ID	Displays the router ID.
AS Summary Link States	Displays the summary LSA information in the AS.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
AdvertisingRouter	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.

Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, which can be only 0 now.
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database external** command.

```

FS# show ip ospf database external
      OSPF Device with ID (1.1.1.35) (Process ID 1)
        AS External Link States
LS age: 752
Options: 0x2 (*|---|E|)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 0

```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-5 AS External Link States	Displays autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Indicates the external link type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.

Forward Address

IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.

External Route Tag

External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used by other routing processes to redistribute OSPF routes.

The following example displays the output of the **show ip ospf database network** command:

```
FS# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
Options:0x2 (*|---|E|)
LS Type:network-LSA
Link State ID:192.88.88.27 (address of Designated Router)
Advertising Router:1.1.1.1
LS Seq Number: 80000001
Checksum:0x5366
Length: 32
Network Mask: /24
Attached Router:1.1.1.1
Attached Router:3.3.3.3
```

The following table describes the fields in the output of the **show ip ospf database network** command.

Field	Description
OSPF Router with ID	Displays the router ID corresponding to the follow-up information and the process ID corresponding to the OSPF.
Network LinStates	Displays the network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Device	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the network corresponding to the LSA.
Attached Router	Displays the device that is connected with the network.

The following example displays the output of the **show ip ospf database device** command:

```
FS# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
```

```
Options:0x2 (*|~|~|~|~|E|~)
Flags:0x3 :ABR ASBR
LS Type:router-LSA
Link State ID:1.1.1.1
Advertising Router:1.1.1.1
LS Seq Number: 80000012
Checksum:0x6d3a
Length: 48
Number of Links: 2
Link connected to:Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

The following table describes the fields in the output of the **show ip ospf database device** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Device Link States	Displays the device LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
Flag	Flag
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Number of Links	Displays the number of links associated with the device.
Link connected to	Displays what the link is connected to and the network type.
(Link ID)	Link identifier
(Link Data)	Link data
Number of TOS metrics	TOS value, supporting TOS0 only

TOS 0 Metrics

TOS0 metric

The following example displays the output of the **show ip ospf database summary** command:

```
FS# show ip ospf database summary
```

```
    OSPF Device with ID (1.1.1.1) (Process ID 1)
```

```
        Summary Link States (Area 0.0.0.0)
```

```
LS age: 499
```

```
Options: 0x2 (*-|-|-|E|-)
```

```
LS Type: summary-LSA
```

```
Link State ID: 10.0.0.0 (summary Network Number)
```

```
Advertising Device: 1.1.1.1
```

```
LS Seq Number: 80000004
```

```
Checksum: 0x330e
```

```
Length: 28
```

```
Network Mask: /24
```

```
    TOS: 0   Metric: 11
```

The following table describes the fields in the output of the **show ip ospf database summary** command.

Field	Description
OSPF Router with ID	Displays the router ID.
Summary Net Link States	Displays the summary network LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
TOS	TOS value, supporting only 0 now
Metric	Displays the metric of the route corresponding to the LSA.

The following example displays the output of the **show ip ospf database nssa-external** command:

```
FS# show ip ospf database nssa-external
    OSPF Device with ID (1.1.1.1) (Process ID 1)
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Device: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    NSSA: Forward Address: 100.0.2.1
    External Route Tag: 0
```

The following table describes the fields in the output of the **show ip ospf database nssa-external** command.

Field	Description
OSPF Router with ID	Displays the router ID.
NSSA-external Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option
LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequential number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.

Metric	Displays the metric of the route corresponding to the LSA.
NSSA:Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database external** command:

```

FS# show ip ospf database external
    OSPF Device with ID (1.1.1.1) (Process ID 1)
      AS External Link States
LS age: 1290
Options: 0x2 (*|---|E|)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Device: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0

```

The following table describes the fields in the output of the **show ip ospf database external** command.

Field	Description
OSPF Device with ID	Displays the router ID.
Type-7 AS External Link States	Displays the type 7 autonomous external LSA information.
LS age	Displays the keepalive period of the LSA.
Options	Option

LS Type	Displays the type of the LSA.
Link State ID	Displays the link ID of the LSA.
Advertising Router	Displays the device advertising the LSA.
LS Seq Number	Displays the sequence number of the LSA.
Checksum	Displays the checksum of the LSAs.
Length	Displays the length (in bytes) of the LSA.
Network Mask	Displays the network mask of the route corresponding to the LSA.
Metric Type	Displays the metric type.
TOS	TOS value, which can be 0 only now.
Metric	Displays the metric of the route corresponding to the LSA.
Forward Address	IP address through which traffic is forwarded to the destination network. If this address is 0.0.0.0, the data traffic will be forwarded to the device that generates the link state.
External Route Tag	External route tag. Each external route has a 32-byte route tag. The OSPF does not use the route tag by itself, but it will be used in redistributing OSPF routes by other routing process.

The following example displays the output of the **show ip ospf database database-summary** command:

```
FS# show ip ospf database database-summary
```

```
OSPF process 1:
```

```
Device Link States      : 4
```

```
Network Link States    : 2
```

```
Summary Link States    : 4
```

```
ASBR-Summary Link States : 0
```

```
AS External Link States : 4
```

```
NSSA-external Link States: 2
```

The following table describes the fields in the output of the command **show ip ospf database database-summary**.

Field	Description
OSPF Process	OSPF process ID
Router Link	Number of device LSAs in the area

	Network Link	Number of network LSAs in the area
	Summary Link	Number of summary LSAs in the area
	ASBR-Summary Link	Number of ASBR summary LSAs in the area
	AS External Link	Number of NSSA LSAs in the area
	NSSA-external Link	Number of NSSA LSAs in the area
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.61 show ip ospf interface

	Use this command to display the OSPF-associated interface information.	
	show ip ospf [<i>process-id</i>] interface [<i>interface-type interface-number</i> brief]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID
	<i>interface-type</i>	(Optional) type of the specified interface
	<i>interface-number</i>	(Optional) number of the specified interface
	brief	Displays the summary of the interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command displays the OSPF information on the interface.	
Configuration Examples	The following example displays the output of the show ip ospf interface fastEthernet 0/1 command:	
	<pre>FS# show ip ospf interface fastEthernet0/1 FastEthernet 0/1 is up, line protocol is up Internet Address 192.88.88.27/24, Iindex 4, Area 0.0.0.0, MTU 1500 Matching network config: 192.88.88.0/24 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1 Transmit Delay is 1 sec, State DR, Priority 1,BFD enabled Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27</pre>	

Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:03
 Neighbor Count is 1, Adjacent neighbor count is 1
 Crypt Sequence Number is 70784
 Hello received 1786 sent 1787, DD received 13 sent 8
 LS-Req received 2 sent 2, LS-Upd received 29 sent 53
 LS-Ack received 46 sent 23, Discarded 1

The following table describes the fields in the output of the **show ip ospf interface serial1/0** command.

Field	Description
FastEthernet 0/1 State	State of the network interface; UP means normal working and Down means faults.
Internet Address	Interface IP address
Area	OSPF area of the interface
MTU	Corresponding MTU
Matching network config	Network area configured for the corresponding OSPF
Process ID	Corresponding process ID
Router ID	OSPF router id
Network Type	OSPF network type
Cost	OSPF interface cost
Transmit Delay is	OSPF interface transmit delay
State	DR/BDR state ID
Priority	Priority of the interface
Designated Router(ID)	DR ID of the interface
DR's Interface address	Address of the DR of the interface
Backup designated device(ID)	Router ID of the BRD of the interface
BDR's Interface address	Address of the BDR of the interface
Time intervals configured	Hello, Dead, Wait, and Retransmit intervals of the interface
Hello due in	Time when the previous Hello is sent
Neighbor count	Total number of neighbors
Adjacent neighbor count	Number of Full neighbors
Crypt Sequence Number	The corresponding md5 authentication number of the interface
Hello received send	Statistics on the Hello packets sent and received
DD received send	Statistics on the DD packets sent and received
LS-Req received send	Statistics on the LS request packets sent and received
LS-Upd received send	Statistics on the LS update packets sent and received
LS-Ack received send	Statistics on the LS response packets sent and received

	Discard	Statistics on the discarded OSPF packets	
	BFD enabled	Enables BFD for OSPF.	
Related Commands	Command	Description	
	N/A	N/A	
Platform Description	N/A		

2.62 show ip ospf ispf

	Use this command to display the ISPF calculation count in the OSPF area.																		
	show ip ospf [<i>process-id</i>] ispf																		
Parameter Description	Parameter	Description																	
	<i>process-id</i>	OSPF process ID																	
Defaults	N/A																		
Command Mode	Privileged EXEC mode																		
Usage Guide	This command displays the ISPF calculation count in the OSPF area within the last 30 minutes and total ISPF calculation count by now.																		
Configuration Examples	The following displays the ISPF calculation count in the OSPF area. <pre>FS# show ip ospf 1 ispf</pre> OSPF process 1: <table><tr><td>Area_id</td><td>30min_counts</td><td>Total_counts</td></tr><tr><td>0</td><td>32</td><td>1235</td></tr><tr><td>1</td><td>6</td><td>356</td></tr></table> Field Description: <table><tr><th>Field</th><th>Description</th></tr><tr><td>Area_id</td><td>OSPF area ID.</td></tr><tr><td>30min_counts</td><td>ISPF calculation count in the OSPF area within the last 30 minutes.</td></tr><tr><td>Total_counts</td><td>Total count of ISPF calculation.</td></tr></table>		Area_id	30min_counts	Total_counts	0	32	1235	1	6	356	Field	Description	Area_id	OSPF area ID.	30min_counts	ISPF calculation count in the OSPF area within the last 30 minutes.	Total_counts	Total count of ISPF calculation.
Area_id	30min_counts	Total_counts																	
0	32	1235																	
1	6	356																	
Field	Description																		
Area_id	OSPF area ID.																		
30min_counts	ISPF calculation count in the OSPF area within the last 30 minutes.																		
Total_counts	Total count of ISPF calculation.																		
Related Commands	Command	Description																	
	N/A	N/A																	

Platform	N/A
Description	

2.63 show ip ospf neighbor

	Use this command to display the OSPF neighbor list.	
	show ip ospf [<i>process-id</i>] neighbor [statistics] { [<i>interface-type interface-number</i>] [<i>neighbor-id</i>] } [detail] }	
Parameter Description	Parameter	Description
	detail	(Optional) Displays the neighbor details.
	interface-type interface-number	(Optional) Displays the neighbor information of the specified interface
	neighbor-id	(Optional) Displays the information of the specified neighbor
	statistics	(Optional) Displays the neighbor statistics.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command displays neighbor information usually used to check whether the OSPF is running normally.	
Configuration Examples	The following example displays the output of the show ip ospf neighbor command. <pre> FS# show ip ospf neighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State BFD State Dead Time Address Interface 3.3.3.3 1 Full/BDR Up 00:00:32 192.88.88.72 FastEthernet 0/1 FS# show ip ospf neighbor detail Neighbor 3.3.3.3, interface address 192.88.88.72 In the area 0.0.0.0 via interface FastEthernet 0/1 Neighbor priority is 1, State is Full, 11 state changes DR is 192.88.88.27, BDR is 192.88.88.72 Options is 0x52 (* O -[EA]- - E -) Dead timer due in 00:00:32 Neighbor is up for 05:11:27 Database Summary List 0 Link State Request List 0 Link State Retransmission List 0 Crypt Sequence Number is 0 Thread Inactivity Timer on Thread Database Description Retransmission off </pre>	

Thread Link State Request Retransmission off
 Thread Link State Update Retransmission off
 Thread Poll Timer on
 Graceful-restart helper disabled
 BFD session state up

The following table describes the fields in the output of the **show ip ospf neighbor** command.

Field	Description
Neighbor ID	Neighbor ID
Pri	Neighbor priority (for selection of DR)
State	Neighbor status
Dead Time	Remaining time for the neighbor to enter the Dead status
Address	Interface address of the neighbor
Interface	Interface of the neighbor
interface address	Interface address of the neighbor device
In the area	Displays the area that learns the neighbor.
via interface	Displays the interface that learns the neighbor
Neighbor priority	Priority of the neighbor OSPF
State	OSPF neighbor connection state. FULL means the stable state; DR indicates that the neighbor is the designated device; BDR indicates that the neighbor is the backup designated device; DROTHER indicates that the neighbor is not a DR/BDR. Point-to-point network type has no DR or BDR.
State changes times	Times of state changes
Dead Time	Dead time of the neighbor
DR	Interface address of the DR elected by the neighbor device (that is, the DR field of the Hello packet)
BDR	Interface address of the BDR elected by the neighbor device (that is, the BDR field of the Hello packet)
Options	Hello packet E-bit option, where 0 indicates that the area is a STUB area; 2 indicates that the area is not a STUB area.
Dead timer due in	Dead time of the neighbor device
Neighbor up time	Period from when the device is discovered till now
Database Summary List	Statistics on the neighbor DD packets
LinkState Request List	Statistics on the neighbor LS request packets
LinkState Retransmission List	Statistics on the neighbor re-transmit packets

	Crypt Number	Sequence	Area MD5 authentication code
	Thread Timer	Inactivity	Status of invalid neighbor timer
	Thread Description Retransmission	Database	Status of DD packet timer of the interface
	ThreadLinkState Request Retransmission		Status of LS request packet timer of the interface
	ThreadLinkState Update Retransmission		Status of LS update packet timer of the interface
	Thread Poll Timer		Poll Timer start status of the static neighbor
	Graceful-restart helper		Whether it is able to function as the GR Helper of a specified neighbor
Related Commands	Command	Description	
	N/A	N/A	
Platform Description	N/A		

2.64 show ip ospf route

	Use this command to display the OSPF routes.	
	show ip ospf [<i>process-id</i>] route [count <i>ip-address mask</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID. All OSPF routes will be displayed without an ID specified.
	count	Statistics of various OSPF routes
	<i>ip-address mask</i>	Statistics of routes which have a specified prefix and mask.
Defaults	N/A	
Command Mode	Privileged mode	
Usage Guide	This command displays the OSPF routing information. The count option displays the OSPF routing statistics.	
Configuration	The following example displays the output of the show ip ospf route command.	

Examples	OSPF process 1: Codes: C - connected, D - Discard , O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1 C 192.88.88.0/24 [1] is directly connected, FastEthernet 0/1, Area 0.0.0.1	
	The following table describes the fields in the output of the show ip ospf route command.	
	Field	Description
	codes	Route type and corresponding abbreviation and description
	100.0.0.0/24	Route prefix
	[1]	Route cost
	via	Route next hop and interface
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.65 show ip ospf spf

	Use this command to display the routing count in the OSPF area.	
	show ip ospf [<i>process-id</i>] spf	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command displays the routing counts within the latest 30 minutes in the OSPF area and current routing total counts.	
Configuration Examples	The following example displays the output of the show ip ospf [<i>process-id</i>] spf command: FS# show ip ospf 1 spf OSPF process 1: Area_id 30min_counts Total_counts 0 32 1235	

	1	6	356
	The following table describes the fields in the output of the show ip ospf [process-id] spf command.		
	Field	Description	
	Area_id	OSPF area ID	
	30min_counts	OSPF routing counts within the latest 30 minutes	
	Total_counts	Total counts of the OSPF routing till now	
Related Commands	Command	Description	
	show ip ospf	Displays the OSPF summary.	
Platform Description	N/A		

2.66 show ip ospf summary-address

	Use this command to display the converged route of all redistributed routes.													
	show ip ospf <i>[process-id]</i> summary-address													
Parameter Description	Parameter	Description												
	<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.												
Defaults	N/A													
Command Mode	Privileged EXEC mode													
Usage Guide	This command is valid only on the NSSA ABR, and displays only the routes with local aggregation operations.													
Configuration Examples	The following example displays the output of the show ip ospf summary-address command: <pre>FS# show ip ospf summary-address OSPF Process 1, Summary-address: 172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Summary Address</td><td>IP address to be aggregated</td></tr><tr><td>Summary Mask</td><td>Mask to be aggregated</td></tr><tr><td>Advertise</td><td>Whether to advertise the aggregated route</td></tr><tr><td>Status</td><td>Whether the aggregation range takes effect</td></tr><tr><td>Aggregated subnets</td><td>Number of external routes included in the aggregation range</td></tr></table>		Field	Description	Summary Address	IP address to be aggregated	Summary Mask	Mask to be aggregated	Advertise	Whether to advertise the aggregated route	Status	Whether the aggregation range takes effect	Aggregated subnets	Number of external routes included in the aggregation range
Field	Description													
Summary Address	IP address to be aggregated													
Summary Mask	Mask to be aggregated													
Advertise	Whether to advertise the aggregated route													
Status	Whether the aggregation range takes effect													
Aggregated subnets	Number of external routes included in the aggregation range													

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.67 show ip ospf topology

	Use this command to display topology information for OSPF SPF calculation.	
	show ip ospf [<i>process-id</i> [<i>area-id</i>]] topology [adv-router <i>adv-router-id</i> [<i>router-id</i>]] [<i>self-originate</i> [<i>router-id</i>]]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID.
	<i>area-id</i>	Displayed area ID
	topology	Displays a specified OSPF process and topology information summary of an area.
	adv-router	Displays topology information of a specified device. This specified device must be a directly connected neighbor of the current device.
	self-originate	Displays topology information of the current device.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command helps users to understand OSPF SPF calculation topology information and troubleshoot faults caused by topology planning. If the user enables fast reroute calculation, this command displays information related to fast reroute calculation.	
Configuration Examples	The following example displays the result of the show ip ospf topology command: <pre> FS# show ip ospf topology OSPF Router with ID (1.1.1.1) (Process ID 1) Router Topology States (Area 0.0.0.0) +1.1.1.1 +2.2.2.2 +4.4.4.4 +3.3.3.3 +4.4.4.4 +2.2.2.2 +1.1.1.1 </pre>	

```

+3.3.3.3
+4.4.4.4
+3.3.3.3

+3.3.3.3
+1.1.1.1
+2.2.2.2
+4.4.4.4
+2.2.2.2

```

The following example displays the result of the **show ip ospf topology self-originate** command:

FS# show ip ospf topology self-originate

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Topology States (Area 0.0.0.0)

1.1.1.1

Self to Destination Metric: 0

Parent Node: -

Child Node:2.2.2.2

Primary next-hop: -

Backup next-hop: -

Backup Neighbor: -

2.2.2.2

Self to Destination Metric: 1

Parent Node: 1.1.1.1

Child Node:-

Primary next-hop: FastEthernet 0/1 via 10.0.0.1

Backup next-hop: FastEthernet 0/2 via 10.0.1.1

Backup Neighbor: 2.2.2.2

Neighbor to Destination Metric: 0

Neighbor to Self Metric: 10

Neighbor to Primary Neighbor: 0

Self to Neighbor Metric: 1

The description of every field displayed by **show ip ospf topology self-originate** is as follows:

Field	Description
Self to Destination Metric	Metric from the root node to the current destination node
Parent Node	Parent node of the current destination node
Child Node	Chile node of the current destination node
Primary next-hop	Primary next hop for reaching the current the destination node
Backup next-hop	Backup next hop for reaching the current the destination node
Backup Neighbor	Backup neighbor for reaching the current the destination node
Neighbor to Destination Metric	Metric from the backup neighbor to the current destination node

	Neighbor to Self Metric	Metric from the backup neighbor to the root node
	Neighbor to Primary Neighbor	Metric from the backup neighbor to the primary neighbor
	Self to Neighbor Metric	Metric from the root node to the backup neighbor
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.68 show ip ospf virtual-link

	Use this command to display the OSPF virtual link information.	
	show ip ospf [<i>process-id</i>] virtual-link [<i>ip-address</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	ID of the OSPF process. All OSPF routing processes will be displayed if this parameter is not configured.
	<i>ip-address</i>	Associated ID of a virtual link neighbor
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If no virtual link is configured, the command displays the neighbor status and other related information. The show ip ospf neighbor command does not display the neighbor of the virtual link.	
Configuration Examples	The following is the output of the show ip ospf virtual-links command: <pre>FS# show ip ospf virtual-links Virtual Link VLINK0 to device 1.1.1.1 is up Transit area 0.0.0.1 via interface FastEthernet 0/1 Local address 10.0.0.37/32 Remote address 10.0.0.27/32 Transmit Delay is 1 sec, State Point-To-Point, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:05 Adjacency state Full</pre> The following table describes the fields in the output.	

	Field	Description
	Virtual Link VLINK0 to router	Displays the virtual link neighbors and their status.
	Virtual Link State	Displays the virtual link state.
	Transit area	Displays the transit area of the virtual link.
	via interface	Displays the associated interface of the virtual link.
	Local address	Local interface address
	Remote Address	Peer interface address
	Transmit Delay	Displays the transmit delay of the virtual link.
	State	Interface state
	Time intervals configured	Hello, Dead, Wait, and Retransmit interval of the interface
	Adjacency State	Neighbor state, where FULL means the stable state
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.69 summary-address

	Use this command to configure the aggregate route out of the OSPF routing domain. Use the no form of this command to restore the remove the aggregate route.	
	summary-address <i>ip-address net-mask</i> [not-advertise tag value cost cost]	
	no summary-address <i>ip-address net-mask</i> [not-advertise tag cost]	
Parameter Description	Parameter	Description
	<i>ip address</i>	IP address of the aggregate route
	<i>net-mask</i>	Network mask of the aggregate route
	not-advertise	Does not advertise the aggregate route. If the parameter is not configured, the aggregate route is advertised.
	tag value	Sets the tag value of an aggregate route. The range is from 0 to 4,294,967,295.
	cost cost	Cost value of the aggregate route. The range is from 0 to 16,777,214.
Defaults	No aggregate route is configured by default.	
Command Mode	Routing process configuration mode	

Usage Guide	When routes are redistributed by another routing process into the OSPF routing process, every route is advertised to the OSPF-enabled device separately in external LSAs. If the incoming routes are continuous addresses, the autonomous border device can advertise only one aggregate route, reducing the scale of routing table greatly. Unlike the area range command, the area range command aggregates inter-OSPF-area routes, while the summary-address command aggregates external routes of the OSPF routing domain. For the NSSA, the summary-address command is valid only on the NSSA ABR now, and aggregates only redistributed routes.	
Configuration Examples	The following example generates an external aggregate route 100.100.0.0/16. <pre> FS(config)# router ospf20 FS(config-router)# summary-address 100.100.0.0 255.255.0.0 FS(config-router)# redistribute static subnets FS(config-router)# network 200.2.2.0 0.0.0.255 area 1 FS(config-router)# network 172.16.24.0 0.0.0.255 area 0 FS(config-router)# area 1 nssa </pre>	
Related Commands	Command	Description
	area-range	Configures route convergence on the OSPF area border device.
	redistribute	Redistributes routes of other routing processes.
Platform Description	N/A	

2.70 timers lsa arrival

	Use this command to configure the time delay for the same LSA received. Use the no form of this command to restore the default setting.	
	timers lsa arrival <i>arrival-time</i>	
	no timers lsa arrival	
Parameter Description	Parameter	Description
	<i>arrival-time</i>	Configures the time delay when receiving the same LSA. The range is from 0 to 600000 in the unit of milliseconds.
Defaults	The default is 1000.	
Command Mode	Routing process configuration mode	
Usage Guide	No action is done when the same LSA is received within the specified time.	

Configuration Examples	The following example configures the time delay for the same LSA as 2seconds.	
	<pre>FS(config)# routerospf1 FS(config-router)# timers arrival-time 2000</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF information.
Platform Description	N/A	

2.71 timers pacing lsa-group

	Use this command to configure the LSA grouping and then refresh the whole groups as well as the update interval for the aged link state. Use the no form of this command to restore the default setting.	
	timers pacing lsa-group <i>seconds</i>	
	no timers pacing lsa-group	
Parameter Description	Parameter	Description
	<i>seconds</i>	Parameter used for LSA pacing, checksum calculation, and aging interval. The range is from 10 to 1800 in the unit of seconds.
Defaults	The default is 30.	
Command Mode	Routing process configuration mode	
Usage Guide	Each LSA has its own update and aging time (LSA age). If you update and age LSAs separately, many CPU resources will be consumed. To effectively use CPU resources, you can update LSAs of a device in batches. You can use this command to modify the value of seconds, whose default value is 240 seconds. This parameter needs not to be adjusted often. The optimal group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better.	
Configuration Examples	The following example configures the pacing time as 120 seconds.	
	<pre>FS(config)# deviceospf 20 FS (config-router)# timers paing lsa-group 120</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF information.

Platform	N/A
Description	

2.72 timers pacing lsa-transmit

	Use this command to transmit the LSA grouping updating. Use the no form of this command to restore the default setting.	
	timers pacing lsa-transmit <i>transmit-time transmit-count</i>	
	no timers pacing lsa-transmit	
Parameter Description	Parameter	Description
	<i>transmit-time</i>	Configures the interval of sending the LSA grouping. The range is from 10 to 1000.
	<i>transmit-count</i>	Configures the number of LS-UPD packets per group. The range is from 1 to 200.
Defaults	The default configurations are as follows: Transmit-time: 40 milliseconds. Transmit-count: 1	
Command Mode	Routing process configuration mode	
Usage Guide	If there are a large number of LSAs and the load on the system is heavy, you can properly use the transmit-time and transmit-count to inhibit the flooding LS-UPD packet number in the network. If the CPU and network bandwidth loads are not too much, reduce transmit-time and increase transmit-count to quicken the environment convergence.	
Configuration Examples	The following example sets the interval of sending the LS-UPD packets as 50ms, the packets number as 20. FS(config)# routerospf1 FS(config-router)# timers pacing lsa-transmit 50 20	
Related Commands	Command	Description
	show ip ospf	Displays the OSPF process information, including the router ID.
Platform Description	N/A	

2.73 timers spf

	Use this command to configure the delay for SPF calculation after the OSPF receives the topology change as well as the interval between two SPF calculations. Use the no form of this command to restore the default setting.

	timers spf <i>spf-delay spf-holdtime</i>	
	no timers spf	
Parameter Description	Parameter	Description
	<i>spf-delay</i>	Defines the SPF calculation waiting period in seconds. The range is from 0 to 2147483647. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
	<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds. The range is from 0 to 2147483647. When the waiting time is up but the interval between two calculations is still elapsing, the SPF calculation cannot start.
Defaults	For the FSOS not supporting the <code>timers throttle spf</code> command, the default values are as follows: <i>spf-delay</i>: 5seconds; <i>spf-holdtime</i>: 10 seconds. For the FSOS supporting the <code>timers throttle spf</code> command, by default, the <code>timers spf</code> command takes no effect. <i>Spf-delay</i> depends on the default configuration of the <code>timers throttle spf</code> command.	
Command Mode	Routing process configuration mode	
Usage Guide	Smaller values of <i>spf-delay</i> and <i>spf-holdtime</i> mean that OSPF adapts to the topology change faster, and the network convergence period is shorter, but this will occupy more CPU of the router.  The configurations of the timers spf command and the <code>timers throttle spf</code> command may overwrite each other.	
Configuration Examples	The following example configures the delay and holdover period of the OSPF as 3 and 9 seconds respectively. <pre>FS(config)# deviceospf20 FS(config-router)# timersspf 3 9</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the configuration information of the ospf.
	timers throttle spf	Configures the exponential back off delay for SPF calculation. The command is recommended to replace the <code>timers spf</code> command because it is more powerful.
Platform Description	N/A	

2.74 timers throttle lsa all

	Use this command to configure the exponential back off algorithm for the LSA. Use the no form of this command to restore the default setting.	
	timers throttle lsa all <i>delay-time hold-time max-wait-time</i>	
	no timers throttle lsa all	
Parameter Description	Parameter	Description
	<i>delay-time</i>	Configures the time delay of generating the LSA first. The range is from 1 to 600000.
	<i>hold-time</i>	Configures the minimum interval of refreshing the LSA between the first time and second time. The range is from 1 to 600000.
	<i>max-wait-time</i>	Configures the maximum interval of successive refreshing the LSA., which determines whether the LSA is refreshed successively. The range is from 1 to 600000
Defaults	The default configurations are as follows: Delay-time: 0 millisecond, Hold-time: 5000 milliseconds, Max-wait-time: 5000 milliseconds.	
Command Mode	Routing process configuration mode	
Usage Guide	If high convergence performance is required for the link change, the value of delay-time can be relatively small. if you expect to reduce the CPU consumption, increase appropriately several values.  The value of hold-time cannot be smaller than that of delay-time, and the value of max-wait-time cannot be smaller than that of hold-time.	
Configuration Examples	The following example configures the first delay as 10ms, hold-time as 1second and the longest delay as 5seconds. <pre>FS(config)# routerospf1 FS(config-router)# timers throttle lsa all 10 1000 5000</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the configuration information of the ospf
Platform Description	N/A	

2.75 timers throttle route

	Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the no form of this command to restore the default setting.	
	timers throttle route { inter-area <i>ia-delay</i> ase <i>ase-delay</i> }	
	no timers throttle route { inter-area ase }	
Parameter Description	Parameter	Description
	inter-area	Calculates the inter area routes.
	<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
	ase	Calculates the external routes.
	<i>ase-delay</i>	Defines the delay time of the external route calculation, in the range from 0 to 600,000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.
Defaults	The default values are as follows: ia-delay: 0, ase-delay: 0,	
Command Mode	Routing process configuration mode	
Usage Guide	The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.	
Configuration Examples	The following example sets the .delay time of the inter-area route calculation to one second. <pre>FS(config)# router ospf 1 FS(config-router)# timers throttle route inter-area 1000</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.76 timers throttle spf

	Use this command to configure the topology change information for OSPF, including the delay for SPF calculation as well as the interval between two SPF calculations in routing process configuration mode. Use the no form of this command to restore the default setting.	
	timers throttle spf <i>spf-delay spf-holdtime spf-max-waittime</i>	
	no timers throttle spf	
Parameter Description	Parameter	Description
	<i>spf-delay</i>	Defines the SPF calculation waiting period, in the unit of milliseconds, in the range from 1 to 600,000. After receiving the topology change, the OSPF routing process must wait for the specified period to start the SPF calculation.
	<i>spf-holdtime</i>	Defines the interval between two SPF calculations in seconds in the range from 1 to 600,000.
	<i>spf-max-waittime</i>	Defines the maximum interval between two SPF calculations, in milliseconds in the range from 1 to 60,000.
Defaults	The default configurations are as follows: spf-delay: 1000ms; spf-holdtime: 5000ms; spf-max-waittime: 10000ms.	
Command Mode	Routing process configuration mode	
Usage Guide	The spf-delay parameter indicates the delay time of the topology change to the SPF calculation. The spf-holdtime parameter indicates the minimum interval between two SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval until it reaches to spf-max-waittime. If the interval between two SPF calculations has exceeded the required value, the SPF calculation will restart from spf-holdtime. Smaller spf-delay and spf-holdtime values can make the topology converge faster. A greater spf-max-waittime value can reduce the system resource consumption of SPF calculation. Those configurations can be flexibly adjusted according to the actual stability of the network topology. Compared with the timers spf command, this command is more flexible. It speeds up the SPF calculation convergence, and reduces the system resource consumption of SPF calculation due to the topology change. To this end, the timers throttle spf command is recommended.  The value of spf-holdtime cannot be smaller than the value of spf-delay, or the value of spf-holdtime will be set to be equal to the value of spf-delay; The value of spf-max-waittime cannot be smaller than the value of spf-holdtime, or the value of spf-max-waittime will be set to be equal to the value of spf-holdtime automatically; The configurations of the timers spf command and the timers throttle spf command may overwrite each other. If both the timers spf command and the timers throttle spf command are not configured, the default value of the timers throttle spf command is used.	
Configuration Examples	The following example configures the delay and holdtime and the maximum time interval of the OSPF as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the SPF calculation intervals are: 5ms, 1second, 3 seconds, 7 seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90seconds... <pre>FS(config)# routerospf20</pre>	

	FS(config-router)# timersspf 5 1000 90000	
Related Commands	Command	Description
	show ip ospf	Displays the configuration information of OSPF
	timers spf	Configures the SPF calculation delay. This command is supported in versions earlier than FSOS 10.4. It is recommended to replace the timers spf command with the timers throttle spf command.
Platform Description	N/A	

2.77 two-way-maintain

	Use this command to enable the OSPF two-way-maintain function. Use the no form of this command to disable this function.	
	two-way-maintain	
	no two-way-maintain	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	In the large-scale network, partial packets delay or dropped may exist due to much CPU and memory are occupied caused by lots of packet transmission. If the Hello packets are handled over dead-interval, the corresponding adjacency will be disconnected. In this case, you can enable the two-way-maintain function for the packets such as DD, LSU, LSR and LSAck packets from a neighbor in the network (except for the Hello packets), avoiding the neighbor invalidation caused by delayed or dropped Hello packets.	
Configuration Examples	The following example disables the OSPF two-way-maintain function. <pre>FS(config)# routerospf1 FS(config-router)# notwo-way-maintain</pre>	
Related Commands	Command	Description
	show ip ospf	Displays the configuration information of the OSPF
Platform Description	N/A	

3 OSPFv3 Commands

3.1 area authentication

	Use this command to configure OSPFv3 area authentication. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> authentication ipsec spi <i>spi</i> [md5 sha1] [0 7] <i>key</i>	
	no area <i>area-id</i> authentication	
Parameter Description	Parameter	Description
	<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.
	<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
	md5	Specifies a message digest 5 (MD5) authentication mode.
	sha1	Specifies a secure hash algorithm 1 (SHA1) authentication mode.
	0	Indicates that a key is displayed in a plain-text format.
	7	Indicates that a key is displayed in a cipher-text format.
	<i>key</i>	Specifies an authentication key.
Defaults	Authentication is not performed by default.	
Command Mode	Routing process configuration mode	
Usage Guide	FSOS supports three authentication modes: ● null authentication mode, which is configured when authentication is not needed ● MD5 authentication mode ● SHA1 authentication mode If OSPFv3 area authentication is configured, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Interface authentication configuration, however, takes precedence over area authentication configuration.	
Configuration Examples	The following example specifies MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. <pre>FS(config-router)# area 1 authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</pre>	
Related Commands	Command	Description
	ipv6 ospf authentication	Specifies interface authentication.
	area virtual-link authentication	Specifies virtual link authentication.
Platform Description	N/A	

3.2 area default-cost

	Use this command to set the cost of the default route for the ABR in the stub/NSSA area. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> default-cost <i>cost</i>	
	no area <i>area-id</i> authentication	
Parameter Description	Parameter	Description
	<i>area-id</i>	Area ID of the stub/NSSA area. It can be an integer or an IPv4 prefix.
	<i>cost</i>	Cost of the default route of the stub/NSSA area in the range from 0 to 16777215.
Defaults	The default cost is 1.	
Command Mode	Routing process configuration mode.	
Usage Guide	This command can only work in the ABR connected to the stub area.	
Configuration Examples	The following example sets the cost of the default route of stub/NSSA area 50 to 100. <pre> ipv6 router ospf 1 area 50 stub area 50 default-cost 100 </pre>	
Related Commands	Command	Description
	area stub	Sets a stub area.
Platform Description	N/A	

3.3 area encryption

	Use this command to enable encryption authentication for an OSPFv3 area. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> encryption ipsec spi <i>spi</i> esp null [md5 sha1] [0 7] <i>key</i>	
	no area <i>area-id</i> encryption	
Parameter Description	Parameter	Description
	<i>area-id</i>	Specifies an area ID. It can be an integer or the prefix of an IPv4 address.

	<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
	null	Specifies the null encryption mode.
	md5	Specifies the MD5 authentication mode.
	sha1	Specifies the SHA1 authentication mode.
	0	Indicates that a key is displayed in the plain-text format.
	7	Indicates that a key is displayed in the cipher-text format.
	<i>Key</i>	Specifies an authentication key.
Defaults	Encryption authentication is not performed by default.	
Command Mode	Routing process configuration mode	
Usage Guide	FSOS supports the null encryption mode and two authentication modes: MD5 and SHA1. If encryption authentication is configured for an OSPFv3 area, the configuration takes effect on all interfaces (except for those of virtual links) in the area. Encryption authentication configuration on interfaces, however, takes precedence over that of the OSPFv3 area.	
Configuration Examples	The following example specifies null encryption and MD5 authentication for area 1 where OSPFv3 routing processes reside, and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaa. FS(config-router)# area 1 encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaa	
Related Commands	Command	Description
	ipv6 ospf encryption	Specifies interface encryption authentication.
	area virtual-link encryption	Specifies virtual link encryption authentication.
Platform Description	N/A	

3.4 area nssa

	Use this command to configure an NSSA area. Use the no form of this command to remove the NSSA area configuration.	
	area <i>area-id</i> nssa [no-redistribution] [default-information-originate [metric <i>value</i>] [metric-type <i>type</i>]] [no-summary] [translator [stability-interval <i>seconds</i> always]]	
	no area <i>area-id</i> nssa [no-redistribution] [default-information-originate [metric] [metric-type]] [no-summary] [translator [stability-interval always]]	
Parameter Description		
	<i>area-id</i>	ID of the NSSA area.
	no-redistribution	(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal

		areas, but not into the NSSA area.
	default-information-originate	(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).
	metric <i>value</i>	(Optional) Specifies the OSPF default LSA metric. The range is from 0 to 16,777,214, and the default value is 1.
	metric-type <i>type</i>	(Optional) Specifies the OSPF metric type for default routes. The value can be 1 or 2 and the default value is 2.
	no-summary	(Optional) Allows an area to be an NSSA but not have summary routes injected into it.
	translator	(Optional) Configures the NSSA ABR translator.
	stability-interval <i>seconds</i>	(Optional) Configures the stability interval after the role of an NSSA ABR is changed from translator to non-translator. The range is from 0 to 2,147,483,647, the default value is 40 and the unit is second.
	always	(Optional) Configures the NSSA ABR to be always translator. The default NSSA ABR is a non-translator.
Defaults	No NSSA area is defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	The default-information-originate parameter is used to generate a default Type 7 LSA. There is a small difference between NSSA ABR and NSSA ASBR on which this command can take effect. On the ABR, the Type-7 default route generates no matter whether a default route exists in the routing table, while on the ASBR, the Type-7 default route generates only when a default routes exists in the routing table. The no-redistribution parameter is used when the router is an NSSA Area Border Router (ABR) and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area. This parameter is generally used on the device acting as both ASBR and ABR in NSSA area to prevent the routes from being imported into the NSSA area. The no-summary parameter allows an area to be an NSSA but not have summary LSAs injected into it. In an NSSA area involving two or more ABR devices, by default, the ABR of larger router ID is elected as the translator for Type-7 to Type-5 translation. You can configure the translator always parameter to specify an ABR to be always the translator. When the translator of an ABR device is replaced, the ABR still has the translation capability within the stability-interval time. After the stability-interval timer expires and the ABR is not elected as the translator again, then the LSAs translated from Type-7 to Type-5 will be removed from the AS. To prevent route loop, the Type-5 LSAs aggregated by the Type-7 are removed once the ABR device loses the translator capability, instead of waiting for the stability-interval expiration. It is recommended to configure the translator always parameter on only one ABR device in an NSSA area.	
Configuration Examples	The following example sets the area 1 as an NSSA area. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# area 1 nssa</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.5 area-range

	Use this command to set the range of the converged inter-area addresses. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> range <i>ipv6-prefix/prefix-length</i> [advertise not-advertise]	
	no area <i>area-id</i> range <i>ipv6-prefix/prefix-length</i>	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the area in which the addresses are converged. It can be an integer or an IPv4 prefix.
	<i>ipv6-prefix/prefix-length</i>	Range of the converged addresses.
	advertise	Advertises the range of converged addresses.
	not-advertise	The range of the converged addresses is not advertised. By default, the function is enabled.
Defaults	No converged inter-area address range is defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. This command applies only to ABR. Use this command to converge multiple routes of an area into one route and advertise it to other areas. The routing information combination only takes place on the area border. The specific routing information is seen on the intra-area routers, but only one converged route can be seen on the devices in other areas. By configuring the two options of advertise and not-advertise, you can decide whether to advertise the convergence range to enable blocking and filtering. By default, the range is advertised to the outside. The option cost can be used to set the metric value of convergence routing. A number of route convergence commands can be defined. In this way, the number of the routes in the OSPF AS is reduced. Particularly for a large network, the forwarding performance will be improved. When a number of routes are converged, and the containment relationship exists between items, the area range converged is determined by the longest match principle.	
Configuration Examples	The following example converges the routes in area 1. <pre>ipv6 router ospf 1 area 1 range 2001:abcd:1:2::/64</pre>	

Related Commands	Command	Description
	summary-prefix	Sets the range of the external routes to be converged.
Platform Description	N/A	

3.6 area stub

	Use this command to create a stub area or set its attributes. Use the no form of this command to restore the default setting.	
	area area-id stub [no-summary]	
	no area area-id stub [no-summary]	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the stub area. It can be an integer or an IPv6 prefix.
	no-summary	This option applies only to the ABR in the stub area, indicating that the ABR only advertises the type 3 LSA indicating the default route to the stub area, not other type 3 LSAs.
Defaults	No stub area is defined by default.	
Command Mode	Routing process configuration mode	
Usage Guide	If an area is at the end of an entire network, it can be designed as the stub area, in which all the routers must execute the area stub command. If the area is designed as the stub area, it cannot learn the AS external routing information (type 5 LSAs). In practical application, the external routing information takes a large proportion of the link state database, so the devices in the stub area can only learn very little routing information, thus reducing the system resources required for the running of the OSPFv3 protocol. By default, a type 3 LSA advertisement indicating default routing on the ABR in the stub area is generated, then the devices in the stub area can get to the outside of the AS. If a totally stub area needs to be configured, just select the keyword no-summary when executing the area stub command on the ABR.	
Configuration Examples	The following example enables the ABR in stub area 10 to advertise the default route to the stub area. <pre>ipv6 router ospf 1 area 10 stub area 10 stub no-summary</pre>	

Related Commands	Command	Description
	area default-cost	Sets the cost of the default route in the stub area.
Platform Description	N/A	

3.7 area virtual-link

	Use this command to create a virtual link or set its parameters. Use the no form of this command to restore the default setting.	
	area <i>area-id</i> virtual-link <i>router-id</i> [hello-interval <i>seconds</i>] [dead-interval <i>seconds</i>] [retransmit-interval <i>seconds</i>] [transmit-delay <i>seconds</i>] [instance <i>instance-id</i>] [authentication ipsec spi <i>spi</i> [md5 sha1] [0 7] <i>key</i>] [encryption ipsec spi <i>spi</i> esp null [md5 sha1] [0 7] <i>key</i>]	
	no area <i>area-id</i> virtual-link <i>router-id</i> [hello-interval] [dead-interval] [retransmit-interval] [transmit-delay] [instance] [authentication] [encryption]	
Parameter Description	Parameter	Description
	<i>area-id</i>	ID of the area in which the virtual link is located. It can be an integer or an IPv6 prefix.
	<i>Router-id</i>	Neighbor router ID of the virtual link.
	hello-interval <i>seconds</i>	Sets the interval to send the hello message on the local virtual link interface in the range from 1 to 65535 in the unit of seconds.
	dead-interval <i>seconds</i>	Interval for the local interface of the virtual link to wait before considering that the neighbor fails. It is in the range from 1 to 65535 in the unit of seconds.
	retransmit-interval <i>seconds</i>	Interval for retransmitting LSA on the local interface of the virtual link . The range is from 1 to 65535 in the unit of seconds.
	transmit-delay <i>seconds</i>	Delay on the local interface of the virtual link in sending LSA. The range is from 1 to 65535 in the unit of seconds.
	instnace <i>instance-id</i>	Specifies the instance corresponding to the virtual link. No virtual link can be established between different instances. Range: 0.-255
	authentication ipsec spi <i>spi</i> [md5 sha1] [0 7] <i>key</i>	Specifies OSPFv3 authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.

	encryption ipsec spi spi esp null [md5 sha1] [0 7] key	Specifies OSPFv3 encryption authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. null specifies the null encryption mode. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.
	authentication ipsec spi spi [md5 sha1] [0 7] key	Specifies OSPFv3 authentication.  Authentication configuration on two neighboring devices must be consistent. The service password-encryption command enables a key to be displayed in the cipher-text format. <i>spi</i> specifies a security parameter index, in the range from 256 to 4294967295. md5 specifies the MD5 authentication mode. sha1 specifies the SHA1 authentication mode. 0 indicates that a key is displayed in the plain-text format. 7 indicates that a key is displayed in the cipher-text format. <i>key</i> specifies an authentication key.
Defaults	No virtual link is defined by default hello-interval: 10 seconds; dead-interval: four times of the hello-interval; retransmit-interval: five seconds; transmit-interval: one second. Authentication and encryption are not performed by default.	
Command Mode	Routing process configuration mode	
Usage Guide	In the OSPFv3 AS, all the areas must be connected with the backbone area to ensure that they can learn the routes of the whole OSPFv3 AS. If an area cannot be directly connected with the backbone area, it can connect it through a virtual link.  The virtual link shall not be in the stub/NSSA area.  dead-interval, dead-interval and instance shall be configured consistently on both sides of the virtual link neighbors, otherwise neighboring relationship cannot be set up between the virtual neighbors.	
Configuration Examples	The following example configures a virtual link. <pre>FS(config)# ipv6 router ospf 1</pre>	

	FS(config-router)# area 1 virtual-link 192.1.1.1	
Related Commands	Command	Description
	show ipv6 ospf	Displays the OSPFv3 routing process information.
	show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
	show ipv6 ospf virtual-links	Displays the OSPFv3 virtual link information.
Platform Description	N/A	

3.8 auto-cost

	The metric of the OSPFv3 protocol is the interface-based bandwidth. Use this command to enable the bandwidth-based interface metric calculation or modify the reference bandwidth. Use the no form of this command to restore the default setting.	
	auto-cost [reference-bandwidth <i>ref-bw</i>]	
	no auto-cost [reference-bandwidth]	
Parameter Description	Parameter	Description
	reference-bandwidth <i>ref-bw</i>	Reference bandwidth in the range from 1 to 4294967 Mbps.
Defaults	The interface metric is calculated based on the reference bandwidth, which is 100Mbps.	
Command Mode	Routing process configuration mode	
Usage Guide	Use no auto-cost reference-bandwidth to restore it to the default reference bandwidth. You can use ipv6 ospf cost in the interface configuration mode to set the cost of the specified interface, and it takes precedence over the metric calculated based on the reference bandwidth.	
Configuration Examples	The following example changes the reference bandwidth to 10M. <pre> ipv6 router ospf 1 auto-cost reference-bandwidth 5 </pre>	
Related Commands	Command	Description
	ipv6 ospf cost	Sets the cost of an interface.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
Platform Description	N/A	

3.9 bfd all-interfaces

	Use this command to enable the BDF on all OSPFv3 interfaces. Use this command to enable the BDF on all OSPFv3 interfaces in the routing configuration mode. Use the no form of this command to restore the default setting.	
	bfd all-interfaces	
	no bfd all-interfaces	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Routing process configuration mode.	
Usage Guide	The OSPFv3 protocol dynamically discovers the neighbors through the Hello packets. With the BFD function enabled, BFD sessions will be established for the neighbors that match the FULL rules and the status of the neighbors will be detected through the BFD mechanism. Once the BFD neighbor fails, the OSPFv3 will perform the network convergence immediately. You can also use the interface configuration mode command ipv6 ospf bfd [disable] to enable or disable the BFD function on the specified interface, which takes precedence over the command bfd all-interfaces in the routing process configuration mode.	
Configuration Examples	N/A	
Related Commands	Command	Description
	ipv6 router ospf <i>process-id</i>	Enables the OSPFv3 routing process and enter into the routing process configuration mode.
	ipv6 ospf bfd [disable]	Enables or disable the BFD on the specified OSPFv3 interfaces.
Platform Description	N/A	

3.10 clear ipv6 ospf process

	Use this command to clear and restart the OSPF process.
	clear ipv6 ospf { process process-id }

Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID, in the range from 1 to 65535
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	In normal case, it is not necessary to use this command. Use the parameter <i>process-id</i> to clear only one specific OSPFv3 instance. If no <i>process-id</i> is specified, all the OSPFv3 instances will be cleared.	
Configuration Examples	The following example restarts the OSPF process. <pre>enable clear ipv6 ospf process</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.11 default-information originate

	Use this command to generate a default route to the OSPFv3 routing domain in the routing process mode. Use the no form of this command to restore the default setting.	
	default-information originate [always] [metric <i>metric</i>] [metric-type <i>type</i>] [route-map <i>map</i>]	
	no default-information originate [always] [metric] [metric-type] [route-map <i>map</i>]	
Parameter Description	Parameter	Description
	always	(Optional) It makes OSPFv3 generate the default route unconditionally, no matter whether the default route exists locally or not.
	metric <i>metric</i>	(Optional) Initial metric value of the default route, in the range from 0 to 16777214
	metric-type <i>type</i>	(Optional) Type of the default route. There are two type of OSPF external routes: type 1, different metrics seen on different routers; type 2, the same metric seen on different routers.
	route-map <i>map</i>	Associated route-map name, no associated route-map by default
Defaults	No default route is created; The initial metric value is 1;	

	The default route type is type 2.	
Command Mode	Routing process configuration mode	
Usage Guide	When the redistribute or default-information command is executed, the OSPFv3-enabled router automatically turns into the autonomous system border router (ASBR). But the ASBR cannot generate the default route automatically or advertise it to all the routers in the OSPFv3 routing domain. The ASBR generates default routes by default. It is required to configure with the routing process configuration command default-information originate. If the always parameter is used, the OSPF routing process advertises an external default route to the neighbors, no matter whether the default route in the core routing table exists or not. However, the local router does not display the default route. To make sure whether the default route is generated, execute show ipv6 ospf database to observe the OSPF link state database. The execution of the show ipv6 route command on the OSPF neighbor will display the default route. The metric of the external default route can be defined only with the default-information originate command and cannot be set with the default-metric command. There are two types of OSPFv3 external routes: type 1 external routes have changeable routing metrics, while type 2 external routes have constant routing metrics. For two parallel routes with the same route metric to the same destination network, type 1 takes precedence over type 2. As a result, the show ipv6 route command displays only the type 1 route. This command generates a default route of Type-5 LSA, which will not be flooded to the NSSA area. To generate a default route in the NSSA area, use the area nssa default-information-originate command.	
Configuration Examples	The following example generates a default route. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# default-information originate always</pre>	
Related Commands	Command	Description
	redistribute	Redistribute routes.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
	show ipv6 ospf database	Displays the OSPFv3 link state database information.
Platform Description	N/A	

3.12 default-metric

	Use this command to set the default metric for the routes to be redistributed. Use the no form of this command to restore the default setting
	default-metric <i>metric-value</i>
	no default-metric

Parameter Description	Parameter	Description
	<i>metric-value</i>	Default metric for the routes to be redistributed. Its range is from 1 to 16777214.
Defaults	The default is 20.	
Command Mode	The default route type is type 2.	
Usage Guide	This command can be used together with redistribute to set the default metric for the routes to be redistributed. But this command does not apply to two types of routes: ● The default route generated with default-information originate; ● The redistributed direct route, for which 20 is always the default metric value.	
Configuration Examples	The following example sets the default metric for the routes to be redistributed to 10. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# default-metric 10</pre>	
Related Commands	Command	Description
	redistribute	Redistributes the routes.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
Platform Description	N/A	

3.13 distance

	Use this command to set the management distance corresponding to different types of OSPFv3 routes. Use the no form of this command to restore the default setting.	
	distance { <i>distance</i> ospf { intra-area <i>distance</i> inter-area <i>distance</i> external <i>distance</i> } }	
	no distance [ospf]	
Parameter Description	Parameter	Description
	<i>distance</i>	Sets the management distance of the route, in the range from 1 to 255.
	intra-area <i>distance</i>	Sets the management distance of the intra-area route, in the range from 1 to 255.
	inter-area <i>distance</i>	Sets the management distance of the inter-area route, in the range from 1 to 255.
	external <i>distance</i>	Sets the management distance of the external route, in the range from 1 to

	255.				
Defaults	The default value is 110. Management distance of the intra-area route :110, Management distance of the inter-area route :110 Management distance of the external-area route: 110.				
Command Mode	Routing process configuration mode.				
Usage Guide	This command is used to specify different management distances for different types of OSPFv3 routes. The management distance of the route is used for the comparison of routing priority, the smaller the management distance is, the higher the routing priority.  The priority of the route generated by different OSPFv3 processes must be compared using the management distance.  Setting the management distance as 255 indicates the routing entry is unreliable and will not for the packet forwarding.				
Configuration Examples	the following example sets the OSPFv3 external route management distance to 160. <pre>FS(config)# ipv6 router ospf 20 FS(config-router)# distance ospf external 160</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ipv6 router ospf</td><td>Enables the OSPFv3 routing process .</td></tr> </table>	Command	Description	ipv6 router ospf	Enables the OSPFv3 routing process .
Command	Description				
ipv6 router ospf	Enables the OSPFv3 routing process .				
Platform Description	N/A				

3.14 distribute-list in

	Use this command to filter routes that are computed based on Link State Advertisement (LSA). Use the no form of this command to restore the default setting.	
	distribute-list { <i>name</i> prefix-list <i>prefix-list-name</i> } in [<i>interface-type interface-number</i>]	
	no distribute-list { <i>name</i> prefix-list <i>prefix-list-name</i> } in [<i>interface-type interface-number</i>]	
Parameter Description	Parameter	Description
	<i>name</i>	Specifies an ACL filtering rule.
	prefix-list <i>prefix-list-name</i>	Specifies a prefix list filtering rule.
	<i>interface-type interface-number</i>	Specifies an interface on which LSA-based routes are filtered.
Defaults	Routes are not filtered by default.	

Command Mode	Routing process configuration mode	
Usage Guide	Filter the routes computed based on LSA. Only the routes meeting filtering conditions can be forwarded. Route filtering does not affect the link state database and the routing tables of the neighbors. The ACL and prefix list filtering rules cannot be set at the same time. You can set only the ACL filtering rule or the prefix list filtering rule for a specific interface. The routing filtering rules affect only forwarding of local routes but not route computation based on LSA. When route filtering is configured on an ABR, LSA can still compute routes and generate and send inter-area LSAs with prefixes to other areas. This will cause blackhole routes. To prevent the generation of blackhole routes, you can run the area range command with the not-advertise keyword.	
Configuration Examples	The following example filters routes that are computed based on Link State Advertisement (LSA). <pre>FS(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64 FS(config)# ipv6 router ospf 25 FS(config-router)# redistribute rip metric 100 FS(config-router)# distribute-list prefix-list aaa in ethernet 0/1</pre>	
Related Commands	Command	Description
	area range	Configures route aggregation in an area.
Platform Description	N/A	

3.15 distribute-list out

	Use this command to filter routes that are re-distributed. This command has the similar function as the redistribute command. Use the no form of this command to restore the default setting.	
	distribute-list { <i>name</i> prefix-list <i>prefix-list-name</i> } out [bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static]	
	no distribute-list { <i>name</i> prefix-list <i>prefix-list-name</i> } out [bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static]	
Parameter Description	Parameter	Description
	<i>name</i>	Specifies the ACL filtering rule.
	prefix-list <i>prefix-list-name</i>	Specifies the prefix list filtering rule.
	bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static	Specifies the source from which the routes are filtered.
Defaults	Routes are not filtered by default.	

Command Mode	Routing process configuration mode	
Usage Guide	The distribute-list out command has the similar function as the redistribute route-map command. It can be used to filter the routes that are re-distributed based on other protocols into an OSPFv3 area. It does not directly re-distribute routes but works with the redistribute command to re-distribute routes. The ACL and prefix list filtering rules cannot be configured at the same time. You can set only the ACL filtering rule or the prefix list filtering rule to filter the routes from a specific source.	
Configuration Examples	The following example filters static routes that are re-distributed. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# redistribute static subnets FS(config-router)# distribute-list prefix-list jjj out static</pre>	
Related Commands	Command	Description
	redistribute	Re-distributes routes that are carried by other routing processes.
Platform Description	N/A	

3.16 enable mib-binding

	Use this command to bind MIB to a specific OSPFv3 process. Use the no form of this command to restore the default setting.	
	enable mib-binding	
	no enable mib-binding	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	MIB is bound to an OSPFv3 process with the smallest process number by default.	
Command Mode	Routing process configuration mode	
Usage Guide	OSFPv3 MIB has no configuration information about OSFPv3 processes. You can operate only one OSFPv3 process through SNMP. OSFPv3 MIB is bound to the OSFPv3 process with the smallest process number by default. Users' operations take effect on this process. To operate a specific OSFPv3 process through SNMP, you can bind OSFPv3 MIB to the process.	

Configuration Examples	The following example enables users to operate the OSPFv3 process with the process number of 100 through SNMP.	
	<pre>FS(config)# ipv6 router ospf 100 FS(config-router)# enable mib-binding</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays global OSPFv3 configuration information.
	enable traps	Enables the OSPFv3 trap function.
Platform Description	N/A	

3.17 enable traps

	OSPFv3 processes support eight types of trap information, which are classified into two categories. Use this command to send specific trap information. Use the no form of this command to restore the default setting.		
	enable traps [error [IfConfigError IfRxBadPacket VrtIfConfigError VrtIfRxBadPacket] state-change [IfStateChange NbrStateChange NssaTranslatorStatusChange VrtIfStateChange VrtNbrStateChange]]		
	no enable traps [error [IfConfigError IfRxBadPacket VrtIfConfigError VrtIfRxBadPacket] state-change [IfStateChange NbrStateChange NssaTranslatorStatusChange VrtIfStateChange VrtNbrStateChange]]		
Parameter Description	Parameter	Description	
	Error	Configures all error-related trap types. This keyword can also specify the following types of error traps:	
		IfConfigError	Specifies an interface parameter error;
		IfRxBadPacket	Specifies incorrect packets received by an interface;
		VrtIfConfigError	Specifies a parameter error on a virtual interface;
		VrtIfRxBadPacket	Specifies incorrect packets received by a virtual interface.
	state-change	Configures all traps related to state change. This keyword can also specify the following traps related to state change:	
		IfStateChange	Specifies state change of an interface;
		NbrStateChange	Specifies state change of a neighbor;
		NssaTranslatorStatusChange	Specifies status change of the NSSA translator.
		VrtIfStateChange	Specifies state change of a virtual

			interface;
		VirtNbrStateChange	Specifies state change of a virtual neighbor.
Defaults	All traps are disabled by default.		
Command Mode	Routing process configuration mode		
Usage Guide	Before configuring this command, you must run the snmp-server enable traps ospf command; otherwise, OSPFv3 trap information cannot be sent correctly. This is because the function of this command is restricted by the snmp-server command. You can synchronously enable the trap function of different processes even if MIB is not bound to these processes.		
Configuration Examples	The following example enables all traps of OSPFv3 process 100. <pre>FS(config)#ipv6 router ospf 100 FS(config-router)# enable traps</pre>		
Related Commands	Command	Description	
	show ipv6 ospf	Displays global OSPFv3 configuration information.	
	enable mib-binding	Binds MIB to an OSPFv3 process.	
	snmp-server enable traps ospf	Enables OSPFv3 to send trap information.	
Platform Description	N/A		

3.18 graceful-restart

	Use this command to enable the OSPFv3 graceful restart (GR) function and to set the GR period. Use the no form of this command to restore the default setting.	
	graceful-restart [grace-period <i>grace-period</i> inconsistent-lsa-checking]	
	no graceful-restart [<i>graceful-period</i>]	
Parameter Description	Parameter	Description
	grace-period <i>grace-period</i>	Configures the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment when OSPFv3 gracefully restarts. The GR period is in the range from 1 to 1800 in the unit of seconds. The default is 120.
	inconsistent-lsa-checking	Configures the topology change detection. Once the topology change is detected, the device will exit GR and finish the convergence,

	This function is enabled by default after GR is enabled.	
Defaults	This function is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	GR is configured based on the OSPFv3 instance. Different instances could be configured with different parameters. Use this command to configure the GR period. The GR period is the longest interval that lasts from the moment when OSPFv3 fails to the moment that OSPFv3 gracefully restarts. In this period, the device will perform link reconstruction to restore OSPFv3. When the GR period expires, OSPFv3 exits GR and finishes regular operation. To enable the GR function and set the GR period to the 120 seconds, use the graceful-restart command. To modify the GR period, use the graceful-restart grace-period command. Topology stability is indispensable for uninterrupted forwarding. If topology changes, OSPFv3 finishes convergence instead of continuing GR to avoid long time interruption 1) Disabling the topology change detection: If the topology cannot converge in time in the hot backup process, the long term forwarding interruption may occur. 2) Enabling the topology change detection: Forwarding interruption may occur but the interruption time is much shorter than the time it takes to disable topology detection. It is not recommended to disable the topology change detection. In some scenario where long term forwarding interruption does not occur, disabling the topology change detection minimizes the forwarding interruption time. The GR function is unavailable when the Fast Hello function is enabled.	
Configuration Examples	The following example enables GR for OSPFv3 instance 1 and sets the GR period to 60 seconds. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# graceful-restart FS(config-router)# graceful-restart grace-period 60</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.19 graceful-restart helper

	Use this command to enable the OSPFv3 graceful restart helper function. Use the no form of this command to disable this function.
	graceful-restart helper disable
	no graceful-restart helper disable
	Use this command configure the topology change detection method of OSPFv3 GR helper. Use the no form of

	this command to cancel the configuration.	
	graceful-restart helper { strict-lsa-checking internal-lsa-checking }	
	no graceful-restart helper {strict-lsa-checking internal-lsa-checking}	
Parameter Description	Parameter	Description
	disable	Disables the device to assist other devices in performing GR.
	strict-lsa-checking	Checks the change of the LSA of types 1-5 and 7 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.
	internal-lsa-checking	Checks the change of the LSA of types 1–3 to judge whether the network topology changes. If the topology changes, the GR helper function will be disabled.
Defaults	The GR helper is enabled by default. The device where the GR helper is enabled does not check the LSA change by default.	
Command Mode	Routing process configuration mode	
Usage Guide	Use this command to enable the GR helper function. When one neighbor device performs graceful restart, the Grace-LSA is advertised to all neighbors. If the device enabled with the GR helper receives the Grace-LSA, it will become the GR Helper to help the neighbors perform GR. The disable option means that it is not allowed to perform the GR helper function for any device in GR. The GR helper does not perform the network change detection by default. The convergence is not performed again until the GR is implemented even if the network changes. Use the strict-lsa-checking or internal-lsa-checking command to enable the device to detect the change of network topology during the GR. The former checks any LSA (types 1-5,7) that stands for the network information, the latter checks the LSA that stands for the AS inner-area route. In the large scale network, it is not recommended to enable the LSA check option because the partial network changes trigger the ending of the GR, decreasing the convergence speed of the entire network.	
Configuration Examples	The following example disables the GF helper function of the OSPFv3 instance 1 and modifies the topology change detection policy. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# graceful-restart helper disable FS(config-router)# no graceful-restart helper disable FS(config-router)# graceful-restart helper strict-lsa-checking</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

3.20 ipv6 ospf area

	Use this command to enable the interface to participate in the OSPFv3 routing process. Use the no form of this command to restore the default setting.	
	ipv6 ospf <i>process-id</i> area <i>area-id</i> [instance <i>instance-id</i>]	
	no ipv6 ospf <i>process-id</i> area [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID.
	area <i>area-id</i>	OSPFv3 area in which the interface participates. It can be an integer or an IPv4 prefix.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	You can use this command to enable the OSPFv3 on an interface, and then configure the OSPFv3 process with ipv6 router ospf. it will be automatically started after this command is used., it will be automatically started after this command is used. Use no ipv6 ospf area to disable the specified interface to participate in the OSPFv3 routing process. Use no ipv6 router ospf to disable all the interfaces to participate in the OSPFv3 routing process. The neighbor relationship can only be established between the routers with the same instance ID. After this command is configured, all the prefix information on the interface will be used in the operation of the OSPFv3.	
Configuration Examples	The following example starts the OSPFv3 process on int fastethernet 0/0 for the specified area of the specified instance. <pre>int fastethernet 0/0 ipv6 ospf 1 area 2 instance 2</pre>	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	passive-interface	Setsthe a passive interface.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
Platform Description	N/A	

3.21 ipv6 ospf authentication

	Use this command to configure OSPFv3 interface authentication. Use the no form of this command to restore the default setting.	
	ipv6 ospf authentication [null ipsec spi <i>spi</i> [md5 sha1] [0 7] <i>key</i>] [instance <i>instance-id</i>]	
	no ipv6 ospf authentication [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	null	Indicates that authentication is not performed.
	<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
	md5	Specifies the MD5 authentication mode.
	sha1	Specifies the SHA1 authentication mode.
	0	Indicates that a key is displayed in the plain-text format.
	7	Indicates that a key is displayed in the cipher-text format.
	<i>key</i>	Specifies an authentication key.
Defaults	Authentication is not performed by default.	
Command Mode	Interface configuration mode	
Usage Guide	FSOS supports three authentication modes: ● null authentication mode, which is configured when authentication is not needed ● MD5 authentication mode ● SHA1 authentication mode  OSPFv3 authentication parameters configured on interconnected interfaces must be consistent.	
Configuration Examples	The following example specifies MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. <pre>FS(config-if)# ipv6 ospf authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa</pre>	
Related Commands	Command	Description
	ipv6 ospf authentication	Specifies interface authentication.
	area virtual-link authentication	Specifies virtual link authentication.
Platform Description	N/A	

3.22 ipv6 ospf bdf

	Use this command to enable or disable the BFD on the specified OSPFv3-enabled interface. Use the no form of

	this command to restore the default setting.	
	ipv6 ospf bfd [disable] [instance <i>instance-id</i>]	
	no ipv6 ospf bfd [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	disable	Disables the BFD function on the specified OSPF interface.
	instance <i>instance-id</i>	Configures the specified OSPFv3 instance on the interface, in the range from 0 to 255.
Defaults	No configuration is made by default. The BFD configuration in the OSPFv3 process configuration mode will apply.	
Command Mode	Interface configuration mode.	
Usage Guide	The command ipv6 ospf bfd in the interface configuration mode takes precedence over the bfd all-interfaces command in the routing process configuration mode. You can use this command to enable the BFD on the specified interface according to the actual environment, also can use the command bfd all-interfaces in the OSPFv3 process configuration mode to enable the BFD function on all OSPFv3 interfaces and use the command ip v6 ospf bfd disable to disable the BFD on the specified interface.	
Configuration Examples	<pre>FS(config)# int fastethernet 0/0 FS(config-if-fastethernet 0/0)# ipv6 ospf bfd</pre>	
Related Commands	Command	Description
	ipv6 router ospf <i>process-id</i>	Starts the OSPFv3 routing process and enter into the routing process configuration mode.
	bfd all-interfaces	Enables the BFD on all OSPFv3 interfaces.
Platform Description	N/A	

3.23 ipv6 ospf cost

	Use this command to set the cost of the interface. Use the no form of this command to restore the default setting	
	ipv6 ospf cost <i>cost</i> [instance <i>instance-id</i>]	
	no ipv6 ospf cost [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	Cost	Cost of interface, in the range from 0 to 65535.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0

		to 255.
Defaults	The default interface cost is the reference bandwidth/Bandwidth (100Mbps by default).	
Command Mode	Interface configuration mode.	
Usage Guide	By default, the cost of the OSPFv3 interface is 100Mbps/Bandwidth, in which the Bandwidth is the bandwidth of the interface and configured with the command bandwidth in the interface configuration mode. The default costs of OSPFv3 interfaces for several typical lines are: ● 64K serial line: 1562; ● E1 line: 48 ● 10M Ethernet: 10 ● 100M Ethernet: 1 The OSPFv3 cost configured with the command ipv6 ospf cost will overwrite the default configuration.	
Configuration Examples	The following example sets the cost of the interface to 1: <pre>FS(config)# int fastethernet 0/0 FS(config-if)# ipv6 ospf cost 1</pre>	
Related Commands	Command	Description
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.
Platform Description	N/A	

3.24 ipv6 ospf dead-interval

	Use this command to set a dead interval of neighbors on an interface. If no hello packet is received from a neighbor within the interval, the neighboring relationship is considered to fail. Use the no form of this command to restore the default setting	
	ipv6 ospf dead-interval { <i>seconds</i> minimal hello-multiplier <i>multiplier</i> } [instance <i>instance-id</i>]	
	no ipv6 ospf dead-interval [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>seconds</i>	Dead interval of neighbors. Its range is from 1 to 65535 in the unit of seconds.

	minimal hello-multiplier <i>multiplier</i>	Enables the fast hello function, which takes 1s as the dead interval of neighbors. <i>Multiplier</i> specifies the number of hello packets sent in one second, in the range from 3 to 20.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.
Defaults	If the fast hello function is not enabled, the dead interval of neighbors is four times longer than the hello interval.  If the hello interval is changed, the dead interval of neighbors varies automatically.	
Command Mode	Interface configuration mode	
Usage Guide	The dead interval of neighbors must be longer than the hello interval. The OSPFv3 fast hello function allows OSPFv3 to fast discovery neighbors and detect whether neighboring relationships are valid. To enable the OSPFv3 fast hello function, you can specify the minimal and hello-multiplier keywords and the <i>multiplier</i> parameter in this command. minimal specifies the deal interval of neighbors to be 1s; hello-multiplier specifies the number of times that hello packets are sent in a second. Therefore, this configuration reduces the hello interval to be shorter than 1s. If an interface is enabled with the fast hello function, the hello-interval field of hello packets to be advertised by this interface is set to 0, and that of hello packets received from this interface is omitted.  dead-interval, minimal, and hello-multiplier that are introduced to enable the fast hello function cannot be configured together with hello-interval. No matter whether the fast hello function is configured, the dead interval of neighbors on the interconnected interfaces of neighbors must be consistent. The values of hello-multiplier on the interconnected interfaces can be different but you must ensure that at least one hello packet is received within the dead interval of neighbors. You can use the show ipv6 ospf interface command to monitor the dead interval of neighbors and the fast hello interval on an interface.	
Configuration Examples	The following example sets the dead interval of neighbors to 60 seconds on an interface. <pre>FS(config)# int fastethernet 0/0 FS(config-if)# ipv6 ospf dead-interval 60</pre>	
Related Commands	Command	Description
	ipv6 ospf hello-interval	Sets the interval for sending the Hello message on an interface.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3

		routing process
Platform	N/A	
Description		

3.25 ipv6 ospf encryption

	Use this command to enable OSPFv3 encryption authentication on an interface. Use the no form of this command to restore the default setting.	
	ipv6 ospf encryption [null ipsec spi spi esp null [md5 sha1] [0 7] key]	
	no ipv6 ospf encryption	
Parameter Description	Parameter	Description
	null	Indicates that encryption authentication is not performed.
	<i>spi</i>	Specifies a security parameter index, in the range from 256 to 4294967295.
	null	Specifies the null encryption mode.
	md5	Specifies the MD5 authentication mode.
	sha1	Specifies the SHA1 authentication mode.
	0	Indicates that a key is displayed in the plain-text format.
	7	Indicates that a key is displayed in the cipher-text format.
	<i>key</i>	Specifies an authentication key.
Defaults	Encryption authentication is not performed by default.	
Command Mode	Interface configuration mode	
Usage Guide	FSOS supports the null encryption mode and two authentication modes: MD5 and SHA1.	
	 OSPFv3 encryption authentication parameters configured on interconnected interfaces must be consistent.	
Configuration Examples	The following example specifies null encryption and MD5 authentication in OSPFv3 interface configuration mode and sets the authentication password to aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. FS(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	
Related Commands	Command	Description
	area encryption	Specifies area encryption authentication.
	area virtual-link encryption	Specifies virtual link encryption authentication.
Platform	N/A	
Description		

3.26 ipv6 ospf hello-interval

	Use this command to set the interval for the interface to send the Hello message. Use the no form of this command to restore the default setting	
	ipv6 ospf hello-interval <i>seconds</i> [instance <i>instance-id</i>]	
	no ipv6 ospf hello-interval [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for sending the Hello message. Its range is from 1 to 65535 in the unit of seconds.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.
Defaults	The broadcast network and point-to-point network :10 seconds. The point-to-multipoint network and NBMA network :30 seconds.	
Command Mode	Interface configuration mode.	
Usage Guide	The same hello sending intervals must be set for the neighbors, otherwise the normal adjacency cannot be established.  The dead-interval minimal hello-multiplier and hello-interval parameters for Fast Hello cannot be configured simultaneously.	
Configuration Examples	The following example sets the interval for the interface to send the Hello message to 20 seconds. <pre>ipv6 ospf hello-interval 20</pre>	
Related Commands	Command	Description
	ipv6 ospf dead-interval	Sets the interval for the interface to consider that the neighbor fails.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.
Platform Description	N/A	

3.27 ipv6 ospf mtu-ignore

	Use this command to ignore the MTU check when an interface receives the database description message. Use the no form of this command to restore the default setting.
	ipv6 ospf mtu-ignore [instance <i>instance-id</i>]
	no ipv6 ospf mtu-ignore [instance <i>instance-id</i>]

Parameter Description	Parameter	Description
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface, in the range from 0 to 255.
Defaults	The MTU check is enabled by default.	
Command Mode	Interface configuration mode.	
Usage Guide	After receiving the database description message, the OSPFv3 device will check whether the MTU of neighbor interface is the same as its own MTU. If the received database description message indicates an MTU greater than its own interface's MTU, the neighbor relationship cannot be established. This can be fixed by disabling the MTU check.	
Configuration Examples	The following example disables the MTU check function on the ethernet 1/0. <pre>FS(config)# interface ethernet 1/0 FS(config-if)# ipv6 ospf mtu-ignore</pre>	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	ipv6 mtu	Sets the value of IPv6 MTU of the interface.
Platform Description	N/A	

3.28 ipv6 ospf neighbor

	Use this command to configure the OSPFv3 neighbor manually. Use the no form of this command to restore the default setting.	
	ipv6 ospf neighbor <i>ipv6-address</i> [[cost <1-65535>] [poll-interval <0-2147483647> priority <0-255>]] [instance <i>instance-id</i>]	
	no ipv6 ospf neighbor <i>ipv6-address</i> [[cost <1-65535>] [poll-interval < 0-2147483647 > priority < 0-255 >]] [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	cost <i>cost</i>	(Optional) Configures the cost to each neighbor in point-to-multipoint network. It is not defined by default, where the cost configured on the interface will be used. It ranges from 1 to 65535. Only the networks of the point-to-multipoint type support this option.
	poll-interval <i>seconds</i>	(Optional) Interval for polling the neighbors (in seconds), which ranges from 1

		to 2147483647. Only the networks of the non-broadcast (NBMA) type support this option.
	priority <i>priority</i>	(Optional) Configures the priority value of non-broadcast network neighbors, which ranges from 0 to 255. Only the non-broadcast (NBMA) type network supports this option.
	instance <i>instance-id</i>	(Optional) Configures the specific OSPFv3 instance on the interface, which ranges from 0 to 255.
Defaults	No neighbor is defined; Neighbor polling interval: 120 seconds; Priority value of non-broadcast network neighbor: 0.	
Command Mode	Interface configuration mode.	
Usage Guide	You can set relevant parameters for the neighbors depending on the actual network type.	
Configuration Examples	The following example shows how to configure the OSPFv3 neighbor in NBMA network as follows: IPv6 address: fe80::2d0:f8ff:fe22:3533, priority value: 1, polling interval: 150 seconds. <pre>FS(config)# interface fastEthernet 0/1 FS(config-if)# ipv6 ospf network non-broadcast FS(config-if)# ipv6 ospf neighbor fe80::2d0:f8ff:fe22:3533 priority 1 poll-interval 150</pre>	
Related Commands	Command	Description
	ipv6 ospf priority	Sets the priority value of an interface.
	ipv6 ospf network	Sets the network type of an interface.
Platform Description	N/A	

3.29 ipv6 ospf network

	Use this command to set the network type of the interface. Use the no form of this command to restore the default setting.	
	ipv6 ospf network { broadcast non-broadcast point-to-point point-to-multipoint [non-broadcast] } [instance <i>instance-id</i>]	
	no ipv6 ospf network [broadcast non-broadcast point-to-point point-to-multipoint [non-broadcast]] [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	broadcast	Specifies the broadcast network type.
	non-broadcast	Specifies the non-broadcast network type.

	point-to-point	Specifies the point-to-point network type.
	point-to-multipoint	Specifies the point-to-multipoint network type.
	point-to-multipoint non-broadcast	Specifies the point-to-multipoint non-broadcast network type.
	instance instance-id	Configures the specific OSPFv3 instance on the interface with the valid id range from 0 to 255.
Defaults	Point-to-point network type: PPP, SLIP, frame relay point-to-point sub-interface and X.25 point-to-point sub-interface encapsulation. NBMA network type: frame relay(except for the point-to-point sub-interface) and X.25 encapsulation (except for the point-to-point sub-interface) Broadcast network type: Ethernet encapsulation. The point-to-multipoint network type is not the default type.	
Command Mode	Interface configuration mode.	
Usage Guide	You can set the network type of the interface according to the actual link type applied and the topology.	
Configuration Examples	The following example sets the network type of the interface that participates in the OSPFv3 to point-to-point. <pre>ipv6 ospf network point-to-point</pre>	
Related Commands	Command	Description
	ipv6 ospf priority	Sets the interface priority.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.
Platform Description	N/A	

3.30 ipv6 ospf priority

	Use this command to set the interface priority. Use the no form of this command to restore the default setting.	
	ipv6 ospf priority <i>number-value</i> [instance <i>instance-id</i>]	
	no ipv6 ospf priority [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>number-value</i>	The priority of the interface. Its range is from 0 to 255.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface. Its range is from 0 to 255.

Defaults	The default priority is 1.										
Command Mode	Interface configuration mode.										
Usage Guide	In the broadcast network type, it is necessary to elect the DR/BDR. In electing the DR/BDR, the device of a higher priority is preferred. If several devices are of the same priority, the one with the largest router-ID is preferred. The device with the priority level of 0 does not participate in the election of DR/BDR.										
Configuration Examples	The following example disables the interface from being elected as the DR/BDR. <pre>FS(config)# interface ethernet 1/0 FS(config-if)# ipv6 ospf priority 0</pre>										
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ipv6 ospf network</td><td>Sets the network type of an interface.</td></tr> <tr> <td>router-id</td><td>Sets the ID of a router.</td></tr> <tr> <td>show ipv6 ospf interface</td><td>Displays the OSPFv3 interface information.</td></tr> <tr> <td>instance instance-id</td><td>Configures the specific OSPFv3 instance on the interface.</td></tr> </table>	Command	Description	ipv6 ospf network	Sets the network type of an interface.	router-id	Sets the ID of a router.	show ipv6 ospf interface	Displays the OSPFv3 interface information.	instance instance-id	Configures the specific OSPFv3 instance on the interface.
Command	Description										
ipv6 ospf network	Sets the network type of an interface.										
router-id	Sets the ID of a router.										
show ipv6 ospf interface	Displays the OSPFv3 interface information.										
instance instance-id	Configures the specific OSPFv3 instance on the interface.										
Platform Description	N/A										

3.31 ipv6 ospf retransmit-interval

	Use this command to set the interval for the interface to retransmit the LSA. Use the no form of this command to restore the default setting.	
	ipv6 ospf retransmit-interval <i>seconds</i> [instance <i>instance-id</i>]	
	no ipv6 ospf retransmit-interval [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>seconds</i>	Interval for retransmitting the LSA. Its range is from 1 to 65535 in the unit of seconds.
	instance <i>instance-id</i>	Configures the specific OSPFv3 instance on the interface.
Defaults	The default is five seconds.	
Command Mode	Interface configuration mode.	

Usage Guide	To ensure the reliability of the routing information transmission, the LSA sent to the neighbor shall be acknowledged by the neighbor. You can use this command to set the interval for the acknowledgement by the neighbor. If no acknowledgement is received within the specified period, the LSA information will be retransmitted.	
Configuration Examples	The following example sets the interval for retransmitting the LSA to 10 seconds. FS(config)# interface ethernet 1/0 FS(config-if)# ipv6 ospf retransmit-interval 10	
Related Commands	Command	Description
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
	ipv6 ospf area	Sets the interface to participate in the OSPFv3 routing process.
Platform Description	N/A	

3.32 ipv6 ospf subvlan

	Use this command to set the interval for the interface to retransmit the LSA. Use the no form of this command to restore the default setting.	
	ipv6 ospf subvlan [all vid]	
	no ipv6 ospf subvlan	
Parameter Description	Parameter	Description
	all	Indicates that packets are allowed to be sent to all sub VLANs.
	vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Defaults	The default settings take effect only on super VLANs with OSPFv3 disabled.	
Command Mode	Interface configuration mode.	
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when OSPF multicast packets are sent over a super VLAN containing multiple sub VLANs, the OSPF multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the OSPF function does not need to be enabled on a super VLAN. Therefore, the OSPF function is disabled by default. However, in some scenarios, the OSPF function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in	

	configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.
Configuration Examples	The following example sends the OSPF multicast packets to sub VLAN 1024 of super VLAN 300. <pre>FS(config)# interface vlan 300 FS(config-if-VLAN 300)# ipv6 ospf subvlan 1024</pre>

3.33 ipv6 ospf transmit-delay

	Use this command to set the delay on the interface in sending the LSA. Use the no form of this command to restore the default setting.	
	ipv6 ospf transmit-delay <i>seconds</i> [instance <i>instance-id</i>]	
	no ipv6 ospf transmit-delay [instance <i>instance-id</i>]	
Parameter Description	Parameter	Description
	<i>seconds</i>	The delay in sending LSA. Its range is from 1 to 65535 in the unit of seconds.
	instance <i>instance-id</i>	Configures the ID of a specific OSPFv3 instance on the interface, in the range from 0 to 255.
Defaults	The default is one.	
Command Mode	Interface configuration mode.	
Usage Guide	Use this command to set the delay on the interface in transmitting the LSA.	
Configuration Examples	The following example sets the delay on the interface in transmitting the LSA. <pre>FS(config)# interface ethernet 1/0 FS(config-if)# ipv6 ospf transmit-delay 2</pre>	
Related Commands	Command	Description
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
Platform Description	N/A	

3.34 ipv6 router ospf

	Use this command to start the OSPFv3 routing process. Use the no form of this command to restore the default setting.	
	ipv6 router ospf	
	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	
	no ipv6 router ospf <i>process-id</i>	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number. Without the process number configured, it indicates that process 1 is started.
	<i>vrf-name</i>	Specifies the VRF that OSPFv3 process belongs to.
Defaults	No OSPFv3 routing process is started.	
Command Mode	Global configuration mode.	
Usage Guide	After the OSPFv3 process is started, the routing process configuration mode is entered. At present, our products support up to 32 OSPFv3 processes.	
Configuration Examples	The following example starts OSPFv3 process in the specified VRF VPN1. FS(config)# ipv6 router ospf 1 vrf vpn_1	
Related Commands	Command	Description
	ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
Platform Description	N/A	

3.35 ipv6 router ospf max-concurrent-dd

	Use this command to set the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes. Use the no form of this command to restore the default setting.	
	ipv6 router ospf max-concurrent-dd <i>number</i>	
	no ipv6 router ospf max-concurrent-dd	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum concurrent interacting neighbors, in the range from 1 to 65535.

Defaults	The default is 5.				
Command Mode	Global configuration mode				
Usage Guide	When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes can be restricted.				
Configuration Examples	The following example sets the maximum concurrent interacting neighbors allowed in all OSPFv3 routing processes to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device. <pre>FS#conf terminal FS(config)#ipv6 router ospf max-concurrent-dd 4</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>max-concurrent-dd</td><td>Sets the maximum concurrent interacting neighbors in the OSPFv3 processes</td></tr> </table>	Command	Description	max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes
Command	Description				
max-concurrent-dd	Sets the maximum concurrent interacting neighbors in the OSPFv3 processes				
Platform Description	N/A				

3.36 log-adj-changes

	Use this command to enable the logging of adjacency changes. Use the no form of this command to restore the default setting.	
	log-adj-changes	
	no log-adj-changes	
Parameter Description	Parameter	Description
	detail	Displays details of adjacency changes
Defaults	By default, the adjacency state log on the entry of or exit from the FULL state is output.	
Command Mode	Routing process configuration mode	
Usage Guide	N/A	
Configuration	The following example turns on the log of adjacency state change.	

Examples	FS(config)# router ospf 1	
	FS(config)# log-adj-changes detail	
Related Commands	Command	Description
	show ipv6 ospf	Displays the OSPF global configuration information
Platform Description	N/A	

3.37 max-concurrent-dd

	Use this command to set the maximum number of DD packets that can be processed concurrently in the OSPFv3 routing process. Use the no form of this command to restore the default setting.	
	max-concurrent-dd <i>number</i>	
	no max-concurrent-dd	
Parameter Description	Parameter	Description
	<i>number</i>	Maximum number of DD packets that can be processed concurrently, in the range from 1 to 65535.
Defaults	The default is 5.	
Command Mode	Routing process configuration mode.	
Usage Guide	When a router is exchanging data with multiple neighbors at the same time which affects its performance, by configuring this command, the maximum concurrent interacting neighbors allowed in each OSPFv3 instance can be restricted.	
Configuration Examples	The following example sets the maximum concurrent interacting neighbors allowed in the current OSPFv3 routing process to 4. The result is that in the interaction between a large number of neighbors, interactions with up to 4 neighbors are allowed to be initiated on this device concurrently, and interactions initiated by up to 4 neighbors are allowed to be received concurrently. That is, interaction with up to 8 neighbors is allowed on this device.	
	<pre>router ipv6 ospf 1 max-concurrent-dd 4</pre>	
Related Commands	Command	Description
	ipv6 router ospf max-concurrent-dd	Sets the maximum concurrent interacting neighbors allowed in the OSPFv3 processes.

Platform	N/A
Description	

3.38 passive-interface

	Use this command to set the passive interface. Use the no form of this command to restore the default setting.	
	passive-interface { default <i>interface-type interface-number</i> }	
	no passive-interface { default <i>interface-type interface-number</i> }	
Parameter Description	Parameter	Description
	default	Sets all the interfaces to passive ones.
	<i>interface-type interface-number</i>	Sets the specified interface to a passive one.
Defaults	No passive interface is set by default.	
Command Mode	Routing process configuration mode	
Usage Guide	After an interface is set to a passive one, it no longer receives or sends the hello message. This command applies to the interfaces participating in the OSPFv3 but not to the virtual links.	
Configuration Examples	The following example enables only the VLAN1 interface to participate in the OSPFv3 process. <pre>passive-interface default no passive-interface vlan 1</pre>	
Related Commands	Command	Description
	ipv6 ospf area	Configures an interface to participate in the OSPFv3 routing process.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
	show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
Platform	N/A	
Description		

3.39 redistribute

	Use this command to start the route redistribution in order to import the routing information of other routing protocols to the OSPFv3 routing process. Use the no form of this command to restore the default setting.	
	redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static } [{ level-1 level-1-2 level-2 } match { internal external [1 2] nssa-external [1 2] } metric <i>metric-value</i> metric-type {1 2 } route-map <i>route-map-name</i> tag <i>tag-value</i>]	
	no redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> rip static } [{ level-1 level-1-2 level-2 } match { internal external [1 2] nssa-external [1 2] } metric metric-type { 1 2 } route-map <i>route-map-name</i>	

	tag <i>tag-value</i>]	
Parameter Description	Parameter	Description
	bgp	The bgp protocol is redistributed.
	connected	The directly connected route is redistributed.
	isis [<i>area-tag</i>]	The isis is redistributed. The area-tag specifies a particular isis instance.
	ospf <i>process-id</i>	The ospf is redistributed. The process-id specifies a particular ospf instance within the range of 1-65535.
	rip	The rip is redistributed.
	static	The static route is redistributed.
	level-1 level-1-2 level-2	It is used in the IS-IS route redistribution only and redistributes the routes at a specified level. .
	match	It is used in the OSPFv3 route redistribution only and filters specific routes for redistribution; internal: inter-area and intra-area routes. external [1 2]: E1, E2 or all external routes. Nssa-external [1 2]: N1, N2 or all external routes of the NSSA area. All sub-type OSPFv3 routes are redistributed by default.
	metric <i>metric-value</i>	Specifies the metric for the OSPFv3 external 2 LSA with metric-value. Its range is 0 to 16777214.
	metric-type { 1 2 }	Set the metric type for the external route to E-1 or E-2.
	route-map <i>map-map-name</i>	Specifies the routing policy for route redistribution. The name of map-tag can be composed of up to 32 characters. No route-map is associated by default.
	tag <i>tag-value</i>	Specifies the tag value redistributed to the OSPFv3 inner route, in the range of 0 to 4294967295.
Defaults	The function is disabled by default; Metric-type: 2; Level-2 routes are redistributed in the ISIS redistribution OSPFv3 routes of all sub-types are redistributed in the OSPFv3 redistribution No route-map is associated	
Command Mode	Routing process configuration mode	
Usage Guide	When a device supports multiple routing protocols, the coordination between these protocols becomes an important task. The device can run the protocols at the same time, so it should redistribute the protocols. This is applicable to all IP routing protocols. The parameters level-1, level-2 or level-1-2 can be configured in the redistribution of the ISIS routes to indicate the level of the routes in the redistribution. By default, the level-2 ISIS routes are redistributed When redistributing OSPFv3 routes, you can configure <i>match</i> to redistribute the routes.of the corresponding	

	sub-type among the redistributed OSPFv3 routes. All types of OSPFv3 routes are redistributed by default. The <i>match</i> parameter of route-map is specific to the source of routes. The parameters <i>tag</i>, <i>metric</i> and <i>metric-type</i> of the set rule of route-map take precedence over the ones configured for the redistribute command.  The metric value of the route-map associated should be in the range of 0 to 16777214. If the metric value is not in this range, the route cannot be introduced. The rules for the no form of the redistribute command are as follows: If some parameters are specified in the no command, restore their default settings; If no parameters are specified in the no command, delete the whole command. For example, if the configuration is made below: Now modify the configuration with the command no redistribute isis 112 level-2 According to the above rules, the command only restores level-2 to default and level-2 is default per se, so after the above no command is executed, the configuration remains as redistribute isis 112 level-2 To delete the whole command, use the command below													
Configuration Examples	The following example redistributes the direct route and associates route-map test : <pre>ipv6 router ospf 1 redistribute connect metric 10 route-map test</pre> The associated route-map is configured as follows: <pre>route-map test permit 10 match metric 20 set metric 30</pre> The effect of the above configuration is to set the metric value which is 20 of the redistributed routes to 30, and that of other routes to 10													
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>default-information originate</td><td>Sets the default route to be redistributed.</td></tr><tr><td>default-metric</td><td>Sets the default metric for the route to be redistributed.</td></tr><tr><td>summary-prefix</td><td>Sets the converged address range of the external route.</td></tr><tr><td>show ipv6 ospf</td><td>Displays the OSPFv3 routing process information.</td></tr><tr><td>show ipv6 ospf database</td><td>Displays the OSPFv3 link state database information.</td></tr></table>	Command	Description	default-information originate	Sets the default route to be redistributed.	default-metric	Sets the default metric for the route to be redistributed.	summary-prefix	Sets the converged address range of the external route.	show ipv6 ospf	Displays the OSPFv3 routing process information.	show ipv6 ospf database	Displays the OSPFv3 link state database information.	
Command	Description													
default-information originate	Sets the default route to be redistributed.													
default-metric	Sets the default metric for the route to be redistributed.													
summary-prefix	Sets the converged address range of the external route.													
show ipv6 ospf	Displays the OSPFv3 routing process information.													
show ipv6 ospf database	Displays the OSPFv3 link state database information.													
Platform Description	N/A													

3.40 router-id

	Use this command to set the router ID (device ID). Use the no form of this command to restore the default setting.
	router-id <i>router-id</i>
	no router-id

Parameter Description	Parameter	Description
	<i>router-id</i>	ID of the device in the IPv4 address format.
Defaults	The OSPFv3 routing process, the largest IPv4 address of all loopback interfaces is elected as the router ID; If there is no loopback interface with an IPv4 address, the OSPFv3 process will elect the largest IPv4 of all other interfaces as the router ID	
Command Mode	Routing process configuration mode	
Usage Guide	Each device that runs the OSPFv3 process shall be identified with a router ID. Router ID is in the format of IPv4 address. Any IPv4 address can be set as the router ID, but the router ID of every routers in the AS must be unique. If multiple OSPFv3 processes are running on the same device, the router ID of every process must be unique. Note that the change of the router ID results in considerable processing work in the protocol. Therefore, it is not recommended to change any router ID without proper reason. A prompt will be given to ask whether you are sure to modify the router ID. It is recommended that you specify a router ID once an OSPFv3 process starts before configuring other parameters for the process	
Configuration Examples	The following example sets the ID of the device that participates in the OSPFv3 process to 1.1.1.1. <pre>router-id 1.1.1.1</pre>	
Related Commands	Command	Description
	ipv6 ospf priority	Sets the interface priority.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
Platform Description	N/A	

3.41 summary-prefix

	Use this command to configure the converged route outside the OSPFv3 routing domain in the routing process configuration mode. Use the no form of this command to restore the default settings.	
	summary-prefix <i>ipv6-prefix/prefix-length</i> [not-advertise] [tag number] [cost cost]	
	no summary-prefix <i>ipv6-prefix/prefix-length</i> [not-advertise] [tag] [cost]	
Parameter Description	Parameter	Description
	<i>ipv6-prefix/prefix-length</i>	Address range of the converged route
	not-advertise	Does not advertise the converged route to neighbors. Absence of this parameter means to advertise.
	tag number	Tag value redistributed to the OSPFv3 inner route, in the range from 0 to

		4294967295.
	cost cost	Cost value of converged route, in the range from 0 to 16777214.
Defaults	No converged route is configured by default.	
Command Mode	Routing process configuration mode.	
Usage Guide	When routes are redistributed by another routing process into the OSPFv3 routing process, every route is advertised to the OSPFv3-enabled device separately in the form of external link state. If the incoming routes are continuous addresses, the autonomous system border device can advertise only one converged route, thus reducing the scale of routing table greatly. It is different from the area range command. The area range involves the convergence of routes between OSPFv3 areas, while the summary-prefix involves the convergence of external routes of the OSPFv3 routing domain. Configuring the summary-prefix command on the ASBR can perform convergence for only redistributed routes; while configuring this command on the NSSA ABR translator can perform convergence for the redistributed routes and the Type-5 routes translated from Type-7.	
Configuration Examples	The following example configures the external route within the 2001:DB8::/64 to the converged route 2001:DB8::/64 to advertise it. <pre>summary-prefix 2001:DB8::/64</pre>	
Related Commands	Command	Description
	area-range	Configures route convergence between the OSPFv3 areas.
	redistribute	Redistributes the routes in other routing process.
Platform Description	N/A	

3.42 show ipv6 ospf

	Use this command to display the information of the OSPFv3 process.	
	show ipv6 ospf [<i>process-id</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID number.
Defaults	N/A	
Command	Privileged EXEC mode	

Mode		
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the OSPFv3 process. <pre> FS# show ipv6 ospf Routing Process "OSPFv3 (1)" with ID 1.1.1.1 Process uptime is 24 minutes Enable two-way-maintain SPF schedule delay 5 secs, Hold time between SPFs 10 secs Initial LSA throttle delay 0 msec Minimum hold time for LSA throttle 5000 msec Maximum wait time for LSA throttle 5000 msec Lsa Transmit Pacing timer 40 msec, 1 LS-Upd LSA interval 5 secs, Minimum LSA arrival 1000 msec Pacing lsa-group: 30 secs Number of incoming current DD exchange neighbors 0/5 Number of outgoing current DD exchange neighbors 0/5 Number of external LSA 0. Checksum Sum 0x0000 Number of AS-Scoped Unknown LSA 0 Number of LSA originated 11 Number of LSA received 4 Log Neighbor Adjacency Changes : Enabled Number of areas in this router is 2 Area BACKBONE(0) Number of interfaces in this area is 1(1) SPF algorithm executed 4 times Number of LSA 3. Checksum Sum 0x1DDF1 Number of Unknown LSA 0 Area 0.0.0.1 (NSSA) Number of interfaces in this area is 1(1) SPF algorithm executed 5 times Number of LSA 7. Checksum Sum 0x445FE Number of Unknown LSA 0 </pre>	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	default-information originate	Sets the default route to be redistributed.
	default-metric	Sets the default metric for the route to be redistributed.
	<i>router-id</i>	Sets the OSPFv3 routing process ID
	timers spf	Sets the delay and the minimum and maximum

		intervals for the OSPFv3 to perform SPF calculation after receiving the topology change information.
Platform Description	N/A	

3.43 show ipv6 ospf database

	Use this command to display the database information of the OSPFv3 process	
	show ipv6 ospf [<i>process-id</i>] database [<i>lsa-type</i> [<i>adv-router router-id</i>]]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID number
	<i>lsa-type</i>	The LSA types are as follows: NSSA-external-LSA, AS-external-LSAs, Link-LSAs, Inter-Area-Prefix-LSAs, Inter-Area-Router-LSAs, Intra-Area-Prefix-LSAs, Network-LSAs, Router-LSAs If this parameter is not specified, all LSA information will be displayed.
	adv-router <i>router-id</i>	Displays the LSA information generated by the specified router.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the OSPFv3 process database. <pre> FS# show ipv6 ospf database OSPFv3 Router with ID (1.1.1.1) (Process 1) Link-LSA (Interface FastEthernet 1/0) Link State ID ADV Router Age Seq# CkSum Prefix 0.0.0.2 1.1.1.1 197 0x80000001 0x7cd8 0 0.0.0.5 2.2.2.2 206 0x80000001 0x8c86 0 Link-LSA (Interface Loopback 1) Link State ID ADV Router Age Seq# CkSum Prefix 0.0.64.1 1.1.1.1 82 0x80000001 0xb760 0 Router-LSA (Area 0.0.0.0) Link State ID ADV Router Age Seq# CkSum Link 0.0.0.0 1.1.1.1 17 0x80000006 0x62a1 1 0.0.0.0 2.2.2.2 156 0x80000003 0x8653 1 Network-LSA (Area 0.0.0.0) Link State ID ADV Router Age Seq# CkSum </pre>	

	0.0.0.5	2.2.2.2	157 0x80000001 0xf8f6			
	Router-LSA (Area 0.0.0.1)					
	Link State ID	ADV Router	Age	Seq#	CkSum	Link
	0.0.0.0	1.1.1.1	17 0x80000002 0x0529			0
	Inter-Area-Prefix-LSA (Area 0.0.0.1)					
	Link State ID	ADV Router	Age	Seq#	CkSum	
	0.0.0.1	1.1.1.1	77 0x80000002 0x83b4			
	AS-external-LSA					
	Link State ID	ADV Router	Age	Seq#	CkSum	
0.0.0.1	1.1.1.1	1 0x80000001 0x6035			E2	
Related Commands	Command				Description	
	ipv6 router ospf				Starts the OSPFv3 routing process.	
Platform Description	N/A					

3.44 show ipv6 ospf interface

	Use this command to display the OSPFv3 interface information.	
	show ipv6 ospf [<i>process- id</i>] interface [<i>interface-type interface-number</i> brief]	
Parameter Description	Parameter	Description
	<i>interface-type interface-number</i>	Specifies the interface type and interface number.
	<i>process- id</i>	OSPFv3 process ID
	brief	Displays the interface summary.
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the OSPFv3 interface.	
	<pre>FS# show ipv6 ospf interface FastEthernet 1/0 is up, line protocol is up Interface ID 2 IPv6 Prefixes fe80::2d0:22ff:fe22:2223/64 (Link-Local Address) OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0 Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1</pre>	

	Transmit Delay is 1 sec, State BDR, Priority 1 Designated Router (ID) 2.2.2.2 Interface Address fe80::c800:eff:fe84:1c Backup Designated Router (ID) 1.1.1.1 Interface Address fe80::2d0:22ff:fe22:2223 Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 1 Hello received 26 sent 26, DD received 5 sent 4 LS-Req received 1 sent 1, LS-Upd received 3 sent 6 LS-Ack received 6 sent 2, Discarded 0	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
Platform Description	N/A	

3.45 show ipv6 ospf neighbor

	Use this command to display the neighbor information of the OSPFv3 process.	
	show ipv6 ospf [<i>process-id</i>] neighbor [interface-type <i>interface-number</i> [detail]] <i>neighbor-id</i> [detail statistics]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number
	detail	Displays details about the neighbor.
	<i>interface-type interface-number</i>	Interface type and interface number
	<i>neighbor-id</i>	Neighbor's router ID
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following command displays the brief information about the OSPFv3 neighbor. FS# show ipv6 ospf neighbor	

	OSPFv3 Process (1) , 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Interface Instance ID 2.2.2.2 1 Full/DR 00:00:33 FastEthernet 1/0 0 FS# show ipv6 ospf neighbor detail Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c In the area 0.0.0.0 via interface FastEthernet 1/0 Neighbor priority is 1, State is Full, 6 state changes DR is 2.2.2.2 BDR is 1.1.1.1 Options is 0x000013 (- R - - E V6) Dead timer due in 00:00:36 Database Summary List 0 Link State Request List 0 Link State Retransmission List 0 BFD session state up	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	ipv6 ospf area	Enables the interface to participate in the OSPFv3 process.
	area virtual-link	Configures the OSPFv3 virtual link.
	show ipv6 ospf interface	Displays the OSPFv3 interface information.
Platform Description	N/A	

3.46 show ipv6 ospf restart

	Use this command to display the OSPFv3 graceful restart configuration.	
	show ipv6 ospf [<i>process-id</i>] restart	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the restarter status. FS# show ipv6 ospf restart	

	Routing Process is ospf 1 Graceful-restart enabled Restart grace period 120 secs Current Restart status is plannedRestart Current Restart remaining time 50 secs Graceful-restart helper support enabled	
	The following example displays the helper status. FS# show ipv6 ospf restart Routing Process is ospf 1 Neighbor 10.1.1.2, interface addr 10.1.1.2 In the area 0.0.0.0 via interface GigabitEthernet 6/0/0 Graceful-restart helper enabled Current helper status is helping Current helper remaining time 50 secs	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
Platform Description	N/A	

3.47 show ipv6 ospf route

	Use this command to display the OSPFv3 route information.	
	show ipv6 ospf [<i>process-id</i>] route [<i>count</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number.
	count	Total number of OSPFv3 routes
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about OSPFv3 routes. FS# show ipv6 ospf route OSPFv3 Process (1) Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area	

	N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2			
	E1 - OSPF external type 1, E2 - OSPF external type 2		Destination	Metric Next-hop
	E2 2001:DB8:1::/64	1/20	via fe80::c800:eff:fe84:1c, FastEthernet 1/0	
	O 2001:DB8:2::/64	11	via fe80::c800:eff:fe84:1c, FastEthernet 1/0, Area 0.0.0.0	
Related Commands	Command		Description	
	ipv6 router ospf		Starts the OSPFv3 routing process.	
Platform Description	N/A			

3.48 show ipv6 ospf summary-prefix

	Use this command to display the external route convergence information of OSPFv3	
	show ipv6 ospf [process-id] summary-prefix	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the external route convergence information of OSPFv3. FS# show ipv6 ospf summary-prefix OSPFv3 Process 1, Summary-prefix: 2001:db8::/64,Metric 16777215,Type0,Tag0,Match count0,advertise	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	summary-prefix	Configures the converge route outside the OSPFv3 routing domain.
Platform Description	N/A	

3.49 show ipv6 ospf topology

	Use this command to display the topology information about each area of OSPFv3.	
	show ipv6 ospf [<i>process-id</i>] topology [<i>area area-id</i>]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number
	<i>area-id</i>	Area ID
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following command displays the topology information about each area of OSPFv3. <pre> FS# show ipv6 ospf topology OSPFv3 Process (1) OSPFv3 paths to Area (0.0.0.0) routers Router ID Bits Metric Next-Hop Interface 1.1.1.1 B -- 2.2.2.2 EB 1 2.2.2.2/fe80::21a:a9ff:fe41:5b06 GigabitEthernet 0/6 OSPFv3 paths to Area (0.0.0.1) routers Router ID Bits Metric Next-Hop Interface 1.1.1.1 V B -- 2.2.2.2 VEB 1 2.2.2.2/fe80::21a:a9ff:fe41:5b06 GigabitEthernet 0/6 </pre>	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	area range	Configures the address range of the OSPF area.
Platform Description	N/A	

3.50 show ipv6 ospf virtual-links

	Use this command to display the virtual link information of the OSPFv3 process	
	show ipv6 ospf [<i>process-id</i>] virtual-links	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPFv3 process ID number
Defaults	N/A	
Command Mode	Privileged EXEC mode.	
Usage Guide	N/A	
Configuration Examples	The following command displays the information about the OSPFv3 virtual link. <pre> FS# show ipv6 ospf virtual-links Virtual Link VLINK1 to router 2.2.2.2 is down Transit area 0.0.0.1 via interface FastEthernet 1/0, instance ID 0 Local address * Remote address 3333::1/128 Transmit Delay is 1 sec, State Down, Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:08 Adjacency state Full </pre>	
Related Commands	Command	Description
	ipv6 router ospf	Starts the OSPFv3 routing process.
	area virtual-link	Configures the OSPFv3 virtual link.
	show ipv6 ospf neighbor	Displays the OSPFv3 neighbor information.
Platform Description	N/A	

3.51 timers lsa arrival

	Use this command to configure a delay for receiving repeated LSAs. Use the no form of this command to restore the default setting.
	timers lsa arrival <i>arrival-time</i>
	no timers lsa arrival

Parameter Description	Parameter	Description
	<i>arrival-time</i>	Specifies the delay for receiving repeated LSAs. The range is from 0 to 600000 in the unit of milliseconds.
Defaults	The default is 1000.	
Command Mode	Routing process configuration mode	
Usage Guide	Configure the device not to process repeated LSAs received within the specific delay.	
Configuration Examples	The following example sets the delay for receiving repeated LSAs to 2 seconds. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# timers lsa arrival 2000</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays OSPFv3 process information, including identifiers of routing devices.
Platform Description	N/A	

3.52 timers pacing lsa-group

	Use this command to set an LSA group pace interval. Use the no form of this command to restore the default setting.	
	timers pacing lsa-group <i>seconds</i>	
	no timers pacing lsa-group	
Parameter Description	Parameter	Description
	seconds	Specifies the LSA group pace interval. The range is from 10 to 1800 in the unit of seconds. The default value is 30.
Defaults	The default is 30.	
Command Mode	Routing process configuration mode	
Usage Guide	Each LSA has its own lifetime, that is, LSA aging time. An LSA existing for 1800s will be refreshed so that the living time of the LSA will not exceed its aging time. This ensures that normal LSAs are not cleared due to timeout of aging time. If update and aging operations of each LSA are separately computed, a large number of CPU	

	resources will be consumed. To effectively utilize CPU resources, configure the device to group LSAs for uniform refreshment. The time for refreshing a group of LSAs is called an LSA group pace interval. Grouping refreshment is to put the LSAs to be refreshed within an LSA group pace interval into a group and refresh them uniformly. When the number of LSAs is fixed, a longer LSA group pace interval will allow the CPU to process more LSAs when the timer expires for one time. To keep the stability of the CPU, you are recommended not to set an over long LSA group pace interval. This prevents the CPU from processing excessive LSAs when the timer expires each time. If the CPU processes a large number of LSAs each time, it is recommended to shorten the LSA group pace interval. For example, if the database has 10000 LSAs, you need to reduce the LSA group pace interval. If it has only 40 to 100 LSAs, you can adjust the group pace interval to 10 through 20 minutes.	
Configuration Examples	The following example sets the LSA group pace interval to 120 seconds. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)#timers pacing lsa-group 120</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays OSPFv3 configuration information.
Platform Description	N/A	

3.53 timers pacing lsa-transmit

	Use this command to set an interval for sending LSA groups. Use the no form of this command to restore the default setting.	
	timers pacing lsa-transmit <i>transmit-time transmit-count</i>	
	no timers pacing lsa-transmit	
Parameter Description	Parameter	Description
	<i>transmit-time</i>	Specifies the interval for sending LSA groups. The range is from 10 to 1000 in the unit of milliseconds.
	<i>transmit-count</i>	Specifies the number of LS-UPD packets in an LSA group. The range is from 1 to 200.
Defaults	The default transmit-time is 40 and the transmit-count is 1.	
Command Mode	Routing process configuration mode	
Usage Guide	There are usually a lot of LSAs on a network; therefore, the load of the device is very high. Setting proper transmit-time and transmit-count values can restrict flooding of LS-UPD packets on the network. When the CPU load is not high and network bandwidth usage is not large, you can reduce the transmit-time	

	value and increase the transmit-count value to accelerate route convergence.	
Configuration Examples	The following example sets the interval for sending LS-UPDs to 50 milliseconds and the specified 20 packets to be sent each time. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# timers pacing lsa-transmit 50 20</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays OSPFv3 process information.
Platform Description	N/A	

3.54 timers spf

	Use this command to set the delay and interval for the OSPFv3 to calculate SPF after receiving the topology change. Use the no format of this command to restore the default setting.	
	timers spf <i>delay holdtime</i>	
	no timers spf	
Parameter Description	Parameter	Description
	<i>spf-delay</i>	Defines the waiting time for the SPF calculation, which ranges from 0 to 2147483647 seconds. After receiving the topology change information, the OSPF routing process has to waiting for a given period before making the SPF calculation.
	<i>spf-holdtime</i>	Defines the interval between two SPF calculations, which ranges from 0 to 2147483647 seconds. If the interval has not passed even if the waiting time has elapsed, no SPF calculation can be made yet.
Defaults	There are two default situations: 1. The versions earlier than FSOS 10.4 do not support the command timers throttle spf. The system default is timers spf 5 10. 2. The FSOS 10.4 and the later versions do support the command timers throttle spf, where timer spf takes no effect by default. The delay for SPF calculation is subject to the default setting of the command timers throttle spf. Refer to the description of the command.	
Command Mode	Routing process configuration mode	
Usage Guide	The smaller the <i>spf-delay</i> and <i>spf-holdtime</i>, the shorter time the OSPF takes to adapt to the topology change, but the more CPU time will be used of the router.  The timer spf configuration and the timers throttle spf configuration will overwrite each other.	

Configuration	The following example sets the delay and holdtime of the OSPFv3 to 3 seconds and 9 seconds respectively.	
Examples	FS(config)# ipv6 router ospf 20 FS(config-router)# timers spf 3 9	
Related Commands	Command	Description
	clear ipv6 ospf	Restarts part of the function of the OSPFv3.
	show ipv6 ospf	Displays the OSPFv3 routing process information.
	timers throttle spf	Configures the exponential backoff delay of the SPF calculation
Platform Description	N/A	

3.55 timers throttle lsa all

	Use this command to configure an exponential backoff algorithm for generating LSAs. Use the no form of this command to restore the default setting.	
	timers throttle lsa all <i>delay-time hold-time max-wait-time</i>	
	no timers throttle lsa all	
Parameter Description	Parameter	Description
	<i>delay-time</i>	Specifies a shortest LSA generation delay, in milliseconds (the first batch of LSAs is usually generated immediately). The range is from 0 to 600000 in the unit of milliseconds.
	<i>hold-time</i>	Specifies a shortest interval between the first two times of LSA refreshment, in milliseconds. The range is from 1 to 600000 in the unit of milliseconds
	<i>max-wait-time</i>	Specifies a longest interval for consecutive two times of LSA refreshment, in milliseconds. The value is used to determine whether LSAs are refreshed consecutively. The range is from 1 to 600000 in the unit of milliseconds.
Defaults	The default <i>delay-time</i> is 0, <i>hold-time</i> is 5000 and <i>max-wait-time</i> is 5000.	
Command Mode	Routing process configuration mode	
Usage Guide	If high route convergence capability is needed when links are changed, set a small <i>delay-time</i> value. To reduce CPU consumption, you can properly increase the values of the parameters.  The <i>hold-time</i> value cannot be smaller than the <i>delay-time</i> value and must be smaller than or equal to the <i>max-wait-time</i> value.	

Configuration Examples	The following example sets <i>delay-time</i> to 10 milliseconds, <i>hold-time</i> to one second, and <i>max-wait-time</i> to five seconds.	
	<pre>FS(config)# ipv6 router ospf 1 FS(config-router)# timers throttle lsa all 10 1000 5000</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays OSPFv3 process information.
Platform Description	N/A	

3.56 timers throttle route

	Use this command to configure the delay time of route calculation on receiving the ASBR summary LSA and the external summary LSA. Use the no form of this command to restore the default setting.	
	timers throttle route { inter-area <i>ia-delay</i> ase <i>ase-delay</i> }	
	no timers throttle route { inter-area ase }	
Parameter Description	Parameter	Description
	inter-area	Calculates the inter area routes.
	<i>ia-delay</i>	Sets the delay time of the inter-area route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the ASBR summary LSA, the router will not calculate the inter-area routes until the ia-delay time runs out.
	ase	Calculates the external routes.
	<i>ase-delay</i>	Sets the delay time of the external route calculation, in the range from 0 to 600000 in the unit of milliseconds. On receiving the external summary LSA, the router will not calculate the external routes until the ase-delay time runs out.
Defaults	The default <i>ia-delay</i> is 0 and <i>ase-delay</i> is 0.	
Command Mode	Routing process configuration mode	
Usage Guide	The default setting is recommended if the network needs to be fast converged. For the instable network where multiple inter-area and external routes exist, if you want to optimize the route calculation and save the CPU resources, increase the delay time.	
Configuration Examples	The following example sets the delay time of the inter-area route calculation to one second. FS(config)# ipv6 router ospf 1	

	FS(config-router)# timers throttle route inter-area 1000	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.57 timers throttle spf

	Use this command to configure, the delay for SPF calculation as well as the minimum and maximum intervals between two SPF calculations after receiving the topology change information for OSPFv3 in the routing process configuration mode. Use the no form of this command to restore the default setting.	
	timers throttle spf <i>spf-delay spf-holdtime spf-max-waittime</i>	
	no timers throttle spf	
Parameter Description	Parameter	Description
	<i>spf-delay</i>	Specifies an SPF calculation delay after the topology change information is received. The range is from 1 to 600000 in the unit of milliseconds.
	<i>spf-holdtime</i>	Specifies a shortest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.
	<i>spf-max-waittime</i>	Specifies a longest interval between two SPF calculations. The range is from 1 to 600000 in the unit of milliseconds.
Defaults	The default <i>spf-delay</i> is 1000. <i>spf-holdtime</i> is 5000 and <i>spf-max-waittime</i> is 10000.	
Command Mode	Routing process configuration mode.	

Usage Guide	<i>Spf-delay</i> refers to the delay from the topology change to the SPF calculation. <i>Spf-holdtime</i> refers to the minimum interval between the first and the second SPF calculations. Then, the interval of the consecutive SPF calculations is at least twice as the last interval till it reaches to <i>spf-max-waittime</i>. If the interval between two SPF calculations has exceeded the required minimum value, the interval of SPF calculation will re-start from <i>spf-holdtime</i>. Smaller <i>spf-delay</i> and <i>spf-holdtime</i> value can make the topology convergence faster. Greater <i>spf-max-waittime</i> value can reduce the SPF calculations. Those configuration are flexible according to the actual stability of the network topology. Compared with the timers <i>spf</i> command, this command is more flexible. It not only speeds up the SPF convergence calculation, but also reduces the system resources consumption of SPF calculation as the topology changes continuously. Therefore, the timers <i>throttle spf</i> command is recommended.  The <i>spf-holdtime</i> cannot be smaller than <i>spf-delay</i>, or the <i>spf-holdtime</i> will be set to be equal to <i>spf-delay</i>;  The <i>spf-max-waittime</i> cannot be smaller than <i>spf-holdtime</i>, or the <i>spf-max-waittime</i> will be set to be equal to <i>spf-holdtime</i> automatically;  The configuration of the timers <i>spf</i> command and of the timers <i>throttle spf</i> command are overwritten each other.  With neither timers <i>spf</i> command nor timers <i>throttle spf</i> command configured, the default value refers to the default of the timers <i>throttle spf</i> command	
Configuration Examples	The following example configures the delay and holdtime and the maximum time interval of the OSPFv3 as 5ms, 1000ms and 90000ms respectively. If the topology changes consecutively, the time for SPF calculation is: five milliseconds, one second, three seconds, seven seconds, 15 seconds, 31 seconds, 63 seconds, 89 seconds, 179 seconds, 179+90 seconds..... <pre>FS(config)# ipv6 router ospf 20 FS(config-router)# timers spf 5 1000 90000</pre>	
Related Commands	Command	Description
	clear ipv6 ospf	Restarts part of the OSPFv3 function.
	show ipv6 ospf	Displays the routing process information of the OSPFv3
	timers spf	Configures the SPF calculation delay .
Platform Description	N/A	

3.58 two-way-maintain

	Use this command to enable two-way OSPFv3 maintenance. Use the no form of this command to disable this function.
	two-way-maintain
	no two-way-maintain

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Two-way OSPFv3 maintenance is enabled by default.	
Command Mode	Routing process configuration mode	
Usage Guide	Sometimes, there are a lot of sent and received packets on a network, occupying large CPU and memory resources. As a result, some packets cannot be processed immediately or are directly lost. If hello packets from a neighbor cannot be processed within the dead interval of neighbors, the connection with the neighbor will be interrupted due to connection timeout. If two-way OSPFv3 maintenance is enabled and a large number of packets exist on the network, besides hello packets, the two-way neighboring relationship between the device and the neighbor can also be maintained by DD, LSU, LSR, and LSAck packets from the neighbor. This prevents the neighboring relationship from failing due to receiving delay or discarding of hello packets.	
Configuration Examples	The following example disables two-way OSPFv3 maintenance. <pre>FS(config)# ipv6 router ospf 1 FS(config-router)# no two-way-maintain</pre>	
Related Commands	Command	Description
	show ipv6 ospf	Displays global OSPFv3 configuration information.
Platform Description	N/A	

4 IS-IS Commands

4.1 address-family ipv6

	Use this command to enter the address-family ipv6 mode. Use the no form of this command to delete all configurations in the address-family ipv6 .	
	address-family ipv6 [<i>unicast</i>]	
	no address-family ipv6 [<i>unicast</i>]	
Parameter Description	Parameter	Description
	<i>unicast</i>	IPv6 unicast address prefix.
Defaults	By default, no address-family ipv6 is configured.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	This command is used for the IPv6 special configurations. To exit to the IS-IS routing process configuration mode, use the exit-address-family command.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# address-family ipv6 unicast</pre>	
Related Commands	Command	Description
	exit-address-family	Exits the address-family ipv6 mode.
Platform Description	N/A	

4.2 adjacency-check

	Use this command to detect protocols supported by the adjacency in the Hello packets. Use the no form of this command is to cancel this detection.	
	adjacency-check	
	no adjacency-check	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	By default, this detection is enabled.	
Command Mode	IS-IS routing process configuration mode or address-family ipv6 mode	
Usage Guide	N/A	
Configuration Examples	FS(config)# router isis FS(config-router)# adjacency-check FS(config-router)# address-family ipv6 FS(config-router-af)# adjacency-check	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.3 area-password

	Use this command to set the plain-text authentication password for the Level-1 area. Use the no form of this command to cancel the password set.	
	area-password [0 7] <i>password-string</i> [send-only]	
	no area-password [send-only]	
Parameter Description	Parameter	Description
	0	Indicates that the key is displayed in plaintext.
	7	Indicates that the key is displayed in ciphertext.
	<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
	send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticate.
Defaults	By default, no authentication password is set.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-1 areas and include authentication information in these packets before they are sent. All IS-IS devices in an area must be configured with the same password.	

	This command does not take effect if the authentication mode command is executed. You need to first delete the previous command configuration. To delete the password, run the no area-password command. If you run the no area-password send-only command, only the send-only setting is canceled. If you run the area-password psw send-only and no area-password send-only commands in sequence, the configuration is changed to area-password psw.	
Configuration Examples	The following example specifies the authentication in the IS-IS area using the plaintext mode with the password being <i>redgiant</i> and the password applicable to the packets sent only, but not to the packets received. <pre>FS(config)# router isis FS(config-router)# area-password redgiant send-only</pre>	
Related Commands	Command	Description
	domain-password	Sets the Level-2 domain password.
	authentication mode	Specifies the IS-IS authentication mode.
Platform Description	N/A	

4.4 authentication key-chain

	Use this command to specify the key-chain used by the IS-IS authentication. Use the no form of this command to cancel the key-chain specified.	
	authentication key-chain <i>name-of-chain</i> [level-1 level-2]	
	no authentication key-chain <i>name-of-chain</i> [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
	level-1	Specifies the authentication key-chain of the Level-1.
	level-2	Specifies the authentication key-chain of the Level-2.
Defaults	By default, the authentication key-chain is not specified.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	If the key chain command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the authentication mode command at the same time. This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the authentication mode command to set the authentication mode. The length of the password key-string in the key-chain shall not be larger than 80 characters if the plain-text authentication mode is used, otherwise this configuration will fail.	

	Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be replaced by the new specified one. If the Level is not specified, the key-chain will apply to both Level-1 and Level-2. The key-chain specified by this command works on the LSP, CSNP and PSNP packets. The IS-IS will send or receive the password that belongs to this key-chain. There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain.	
Configuration Examples	The following example specifies the authentication in the IS-IS area using the key-chain named <i>kc</i>: <pre>FS(config)# router isis FS(config-router)# authentication key-chain kc level-1</pre>	
Related Commands	Command	Description
	authentication mode	Specifies the IS-IS authentication mode.
	authentication send-only	Specifies the IS-IS authentication applicable to the sent packets only, but not to packets received.
	key-chain	Configures the key-chain.
Platform Description	N/A	

4.5 authentication mode

	Use this command to specify the mode of IS-IS authentication. Use the no form of this command to cancel the specified IS-IS authentication mode.	
	authentication mode { md5 text } [level-1 level-2]	
	no authentication mode { md5 text } [level-1 level-2]	
Parameter Description	Parameter	Description
	md5	Specifies the MD5 authentication mode to use.
	text	Specifies the plain-text authentication mode to use.
	level-1	Specifies the authentication mode taking effect on the Level-1.
	level-2	Specifies the authentication mode taking effect on the Level-2.
Defaults	By default, the authentication mode is not specified.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	To make the key-chain configured by the authentication key-chain command effective, you must use the authentication mode command to specify the authentication mode.	

	If no Level is specified, the authentication mode specified is applicable to both Level-1 and Level-2. When configuring the authentication mode command, if the area-password or domain-password command has been executed to configure the plaintext authentication before, the said commands will be overwritten by the new command. If the authentication mode command has been configured, the area-password or domain-password will not be configured successfully, you need to delete the authentication mode command first.	
Configuration Examples	The following example specifies authentication in the IS-IS area to be the MD5 authentication mode. <pre>FS(config)# router isis FS(config-router)# authentication mode md5 level-1</pre>	
Related Commands	Command	Description
	area-password	Sets the area plaintext authentication password.
	authentication key-chain	Specifies the key-chain used by the IS-IS authentication.
	authentication send-only	Specifies the IS-IS authentication applicable to the packets sent only, but not to the packets received.
	domain-password	Sets the domain plaintext authentication password.
Platform Description	N/A	

4.6 authentication send-only

	Use this command to specify the IS-IS authentication only applicable to the packets sent, but not to the packets received. Use the no form of this command to perform the authentication on the packets received.	
	authentication send-only [level-1 level-2]	
	no authentication send-only [level-1 level-2]	
Parameter Description	Parameter	Description
	level-1	Specifies setting send-only on the Level-1.
	level-2	Specifies setting send-only on the Level-2.
Defaults	By default, this command is not configured. If the IS-IS authentication is configured, the authentication will be performed on the packets both sent and recieved.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	With this command configured, the IS-IS will set the authentication password in the packets sent, however, the authentication will not be performed on the packets received. It can apply to the following two occasions: 1. before deploying the IS-IS authentication for all devices in the network. 2. before changing the authentication	

	password or authentication mode. Before the above two tasks start, you need to configure the authentication send-only command first to make each device perform no authentication on the packets received, so as to avoid the network oscillation caused during the subsequent authentication password deployment. After the deployment of the entire network authentication finished, execute the no isis authentication send-only command to cancel the send-only authentication mode. This command can apply to the plain-text authentication mode and MD5 authentication mode. You can use the authentication mode command to set the authentication mode. If the Level is not specified, the authentication mode specified is applicable to both Level-1 and Level-2.	
Configuration Examples	The following example specifies the authentication in the IS-IS area to be the send-only mode. <pre>FS(config)# router isis FS(config-router)# authentication send-only level-1</pre>	
Related Commands	Command	Description
	authentication key-chain	Specifies the IS-IS authentication key-chain.
	authentication mode	Specifies the mode of IS-IS authentication.
	key-chain	Configures the key-chain.
Platform Description	N/A	

4.7 bfd all-interfaces

	Use this command to configure all interfaces running the IS-IS protocol to conduct BFD link detection. bfd all-interfaces [anti-congestion]	
	Use the no form of this command to configure all interfaces running the IS-IS protocol to not conduct BFD link detection. no bfd all-interfaces [anti-congestion]	
Parameter Description	Parameter	Description
	anti-congestion	IS-IS BFD anti-flapping option
Defaults	The IS-IS support for BFD is disabled on all interfaces by default.	
Command Mode	IS-IS routing process configuration mode	
Default Level	14	
Usage Guide	There are two methods for enabling or disabling the IS-IS support for BFD on interfaces. Method 1: In IS-IS routing process configuration mode, run the [no] bfd all-interfaces [anti-congestion] command	

	to enable or disable the IS-IS support for BFD on all interfaces running the IS-IS protocol. Method 2: In interface configuration mode, run the isis bfd [disable anti-congestion] command to enable or disable the IS-IS support for BFD on a specified interface. In normal cases, the BFD function enables to send detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the BFD function enables to rapidly detect the link exception, and notify a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failure link, thereby implementing fast convergence. With the introduction of some new technologies such as the Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the BFD function allows to rapidly detect a link exception, notify a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and perform link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, an IS-IS neighbor relationship can be rapidly established, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed again, and the process repeats. The route switches between the congested link and other links and flapping occurs. The anti-flapping function can be enabled to prevent route flapping in the case of link congestion. After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor status keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a non-congested link. After the link is restored, that is, congestion is removed, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping. When IS-IS anti-flapping is enabled, the BFD anti-flapping command (bfd up-dampening) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred. For details about how to enable the BFD anti-flapping function on an interface, see the configuration example of the ISIS BFD command.  Before the IS-IS support for BFD is configured, a BFD session must be configured on an interface.  When the BFD anti-flapping command is configured on an interface, if the IS-IS support for BFD is already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.  When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.
Configuration Examples	The following example configures all interfaces running the IS-IS protocol to conduct BFD. <pre>FS(config)# router isis 123 FS(config-router)# bfd all-interface</pre>

4.8 clear clns neighbors

	Use this command to clear all IS-IS neighbor relation tables.
	clear clns neighbors

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used in the condition of needing to refresh the IS-IS neighbor relation table immediately.	
Configuration Examples	The following example clears all IS-IS neighbor relation tables.	
	FS# clear clns neighbors	
Related Commands	Command	Description
	clear isis	Clears all IS-IS data structure.
Platform Description	N/A	

4.9 clear isis *

	Use this command to clear the data structure of all IS-ISs.	
	clear isis *	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used in the condition of needing to refresh the LSP immediately. For example, after executing the area-password and domain-password commands, the previous LSPs still exist in this router, you can use this command to clear these LSPs.	
Configuration Examples	FS# clear isis *	

Related Commands	Command	Description
	clear clns neighbors	Clears all IS-IS neighbors.
Platform Description	N/A	

4.10 clear isis counter

	Use this command to clear various statistics of IS-IS.	
	clear isis [tag] counter	
Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears various statistics of IS-IS.	
	FS# clear isis counter	
Related Commands	Command	Description
	clear isis *	Clears the data structure of all IS-ISs.
Platform Description	N/A	

4.11 default-information originate

	Use this command to generate a default routing information and advertise it by LSP. Use the no form of this command to delete the default routing information from LSP.	
	default-information originate [route-map map-name]	
	no default-information originate [route-map map-name]	
Parameter Description	Parameter	Description
	<i>map-name</i>	(Optional) Associated route-map's name, with the maximum length being 32. By default, the route-map is not associated.

Defaults	By default, there is no default route.				
Command Mode	IS-IS routing process configuration mode or address-family ipv6 mode.				
Usage Guide	The default route is not generated in the Level-2 domain. Use this command to allow the default route to enter the Level-2 domain.				
Configuration Examples	The following example generates a default routing information and advertises it by LSP <pre> FS(config)# router isis FS(config-router)# default-information originate FS(config-router)# address-family ipv6 FS(config-router-af)# default-information originate </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

4.12 distance

	Use this command to set the management distance of the IS-IS routes. Use the no form of this command to restore the default settings.	
	distance <i>my-cost</i>	
	no distance	
Parameter Description	Parameter	Description
	<i>my-cost</i>	Distance value in the range of 1 to 255.
Defaults	By default, the distance is 115.	
Command Mode	IS-IS routing process configuration mode or IS-IS address-family ipv6 configuration mode	
Usage Guide	Use this command to configure the management distance of the IS-IS routes. The shorter the management distance, the more reliable the routing information is.	
Configuration Examples	The following example sets the management distance of the IS-IS routes. <pre> FS(config)# router isis FS(config-router)# distance 100 </pre>	

Related Commands	Command	Description
	isis metric	Sets the metric value of the interface.
Platform Description	N/A	

4.13 domain-password

	Use this command to set the plain-text authentication password of Level-2 domain. Use the no form of this command to cancel the password configured.	
	domain-password [0 7] <i>password-string</i> [send-only]	
	no domain-password [send-only]	
Parameter Description	Parameter	Description
	0	Indicates that the key is displayed in plaintext.
	7	Indicates that the key is displayed in ciphertext.
	<i>password-string</i>	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
	send-only	Indicates that the plaintext authentication password is only used to authenticate sent Hello packets in Level-1 areas. Received Hello packets are not authenticated.
Defaults	By default, no authentication password is set.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Run this command to enable authentication of received LSPs, CSNPs, and PSNPs in Level-2 domains and include authentication information in these packets before they are sent. All IS-IS devices in a Level-2 domain must be configured with the same password. This command does not take effect if the authentication mode command is executed. You need to first delete the previous command configuration. To delete the password, run the no domain-password command. If you run the no domain-password send-only command, only the send-only setting is canceled. If you run the domain-password psw send-only and no domain-password send-only commands in sequence, the configuration is changed to domain-password psw.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# domain-password redgiant</pre>	

Related Commands	Command	Description
	area-password	Sets the plain-text authentication password of Level-1 area.
	authentication mode	Specifies the IS-IS authentication mode.
Platform Description	N/A	

4.14 enable mib-binding

	Use this command to bind MIBs with an IS-IS process. Use the no form of this command to unbind the MIB from the IS-IS process.	
	enable mib-binding	
	no enable mib-binding	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, MIBs are bound with IS-IS process 1.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	By default, MIBs are bound with IS-IS process 1. The IS-IS process support multiple processes. The administrator can use this command to bind MIBs with the IS-IS process.	
Configuration Examples	The following example binds the MIB with an IS-IS process. <pre> FS# configure terminal FS(config)# router isis FS(config-router)# enable mib-binding </pre>	
Related Commands	Command	Description
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	isis hello-interval	Sets the interval of sending Hello packets.
	isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.
Platform Description	N/A	

4.15 enable traps

	Use this command to enable the system to send one or multiple types of IS-IS trap packets. Use the no form of this command to disable the system to send IS-IS trap packets.	
	enable traps { all <i>traps set</i> }	
	no enable traps { all <i>traps set</i> }	
Parameter Description	Parameter	Description
	all	Indicates all types of IS-IS trap packets.
	traps set	Indicates the specified type of IS-IS trap packet.
Defaults	By default, no IS-IS trap is sent.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	There are 18 types of IS-IS packets. The IS-IS packets can be classified into multiple sets. Each set includes several types of trap packets. To enable the system to send the IS-IS trap packet, you need to enable the global IS-IS trap using the snmp-server enable traps isis command, specify the host to receive the IS-IS trap packets, and use the enable traps { all <i>traps set</i> } command to specify the type of IS-IS trap packet to be sent.	
Configuration Examples	The following example enables the system to send all IS-IS trap packets to the host of IP address 192.168.1.1. <pre> FS# configure terminal FS(config)#snmp-server enable traps isis FS(config)#snmp-server host 10.1.1.1 traps version 2c public FS(config)#router isis FS(config-router)# enable traps all </pre>	
Related Commands	Command	Description
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	isis hello-interval	Sets the interval of sending Hello packets.
	isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.
Platform Description	N/A	

4.16 exit-address-family

	Use this command to exit IS-IS address family IPv6 configuration mode and return to IS-IS routing process configuration mode.
	exit-address-family

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	IS-IS address-family IPv6 configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example exits IS-IS address family IPv6 configuration mode. <pre>FS (config-router-af)#exit-address-family FS (config-router)#</pre>	
Related Commands	Command	Description
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	isis hello-interval	Sets the interval of sending Hello packets.
	isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.
Platform Description	N/A	

4.17 graceful-restart

	Use this command to enable the IS-IS GR Restart capability. Use the no form of this command to disable this capability.	
	graceful-restart	
	no graceful-restart	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	IS-IS GR is enabled by default.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Use this command to enable the IS-IS GR Restart capability. As long as the network conditions remain unchanged, IS-IS can be restarted and restored to the pre-restart state without impact on data forwarding.	

Configuration	The following example enables the IS-IS GR Restart capability.	
Examples	<pre>FS(config)# router isis FS(config-router)# graceful-restart</pre>	
Related Commands	Command	Description
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	isis hello-interval	Sets the interval of sending Hello packets.
	isis hello-multiplier	Sets the Hello holdtime multiplier for the IS-IS interface.
Platform	N/A	
Description		

4.18 graceful-restart grace-period

	Use this command to configure the maximal interval for the graceful-restart. Use the no form of this command to restore the default interval.	
	graceful-restart grace-period <i>seconds</i>	
	no graceful-restart grace-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Time interval allowed for the device graceful-restart, in the range of 1 to 65,535 seconds.
Defaults	The default value is 300 seconds.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	N/A	
Configuration	The following example sets the interval of the grace-restart to 40 seconds.	
Examples	<pre>FS(config)# router isis FS(config-router)# graceful-restart grace-period 40</pre>	
Related Commands	Command	Description
	graceful-restart	Enables the IS-IS GR Restart capability.
	show isis graceful-restart	Displays the status information of the IS-IS GR Restart.

Platform	N/A
Description	

4.19 graceful-restart helper disable

	Use this command to disable the IS-IS GR Helper capability. Use the no form of this command to enable this capability.	
	graceful-restart helper disable	
	no graceful-restart helper disable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	IS-IS GR Helper capacity is enabled by default.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	To disable the IS-IS GR Helper capability, execute this command. In this case, the IS-IS will ignore the request of graceful-restarting the device.	
Configuration Examples	The following example disables the IS-IS GR Helper capability. <pre>FS(config)# router isis FS(config-router)# graceful-restart helper disable</pre>	
Related Commands	Command	Description
	graceful-restart	Enables the IS-IS GR Restart capability.
Platform	N/A	
Description		

4.20 hello padding

	Use this command to pad IS-IS Hello packets.	
	hello padding [multi-point point-to-point]	
	Use the no form of this command to cancel the padding of IS-IS Hello packets.	
	no hello padding [multi-point point-to-point]	
Parameter Description	Parameter	Description
	multi-point	Pads Hello packets of the LAN type.
	point-to-point	Pads Hello packets of the P2P type.

Defaults	Padding is enabled for Hello packets of the LAN type and P2P type by default.
Command Mode	IS-IS routing process configuration mode
Default Level	14
Usage Guide	Hello packets can be padded to notify a neighbor of the MTU supported by the local device. You can use this command to set whether to pad all Hello packets sent by the IS-IS process. You can also separately specify the type of Hello packets for padding, for example, you can set not to pad all Hello packets of the LAN type or not to pad all Hello packets of the P2P type. The isis hello padding command is available in interface configuration mode. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the interface is cancelled in interface configuration mode.
Configuration Examples	The following example configures to cancel the padding of Hello packets of the P2P type. <pre>FS(config)# router isis FS(config-router)# no hello padding point-to-point</pre>

4.21 hostname dynamic

	Use this command to replace the System ID of the router with the destination router's hostname. Use the no form of this command to cancel this replacement.	
	hostname dynamic	
	no hostname dynamic	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the hostname dynamic function is disabled.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	With this command configured, the hostname of the destination router replaces the System ID. The System IDs shown in the execution of the command such as show isis database , show isis neighbors are all replaced by the hostname of the destination router.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# hostname dynamic</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.22 ignore-lsp-errors

	Use this command to ignore the LSP checksum errors. Use the no form of this command to not ignore the LSP checksum errors.	
	ignore-lsp-errors	
	no ignore-lsp-errors	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the LSP checksum errors are not ignored.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	When the local IS-IS receives a LSP, it will calculate the checksum of LSP received and compare the calculated checksum with that in the LSP packets. By default, if the checksum in the LSP packets is different from the checksum calculated, this LSP will be discarded without processing. If we execute the ignore-lsp-errors command to ignore the checksum errors, the LSP packets with the incorrect checksum will be processed as the normal packets.	
Configuration Examples	FS(config)# router isis FS(config-router)# ignore-lsp-errors	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.23 ip router isis

	Use this command to enable the IPv4 IS-IS on the specified interface. Use the no form of this command to disable the IPv4 IS-IS routing on the specified interface.	
	ip router isis [tag]	
	no ip router isis [tag]	

Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance name.
Defaults	By default, the Ipv4 IS-IS is disabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to enable the IS-IS IPv4 routing protocol on the interface. The no form of this command disables the IS-IS IPv4 routing. If the no ipv4 unicast-routing is executed in global configuration mode, the IS-IS will disable the IPv4 routing function on all interfaces, namely execute the no ipv4 router isis [tag] on all interfaces automatically, while other IS-IS configurations will remain unchanged.	
Configuration Examples	<pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# ip router isis</pre>	
Related Commands	Command	Description
	ipv6 router isis	Enables the IPv6 IS-IS on the interface.
	router isis	Creates IS-IS instances.
Platform Description	N/A	

4.24 ipv6 router isis

	Use this command to enable the IPv6 IS-IS routing on the specified interface. This command must be configured in the IS-IS configuration. The interface will run on the IS-IS instance named with Tag. If this IS-IS instance is inexistent or this IS-IS instance is not enabled and not initialized, the interface will not enable the IS-IS routing. Use the no form of this command to disable the IPv6 IS-IS routing on the specified interface.	
	ipv6 router isis [tag]	
	no ipv6 router isis [tag]	
Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance name
Defaults	By default, the Ipv6 IS-IS routing is not supported on the interface.	
Command Mode	Interface configuration mode	

Usage Guide	Configure this command to enable the IS-IS IPv6 routing protocol on the interface. The no form of this command disables the IS-IS IPv6 routing. If the no ipv6 unicast-routing is executed in the global configuration mode, the IS-IS will disable the IPv6 routing function on all interfaces, namely execute the no ipv6 router isis [tag] on all interfaces automatically, while other IS-IS configurations will remain unchanged.	
Configuration	FS(config)# interface GigabitEthernet 0/1	
Examples	FS(config-if)# ipv6 router isis	
Related Commands	Command	Description
	ip router isis	Enables the IPv4 IS-IS on the interface.
	router isis	Creates IS-IS instances.
Platform Description	N/A	

4.25 isis authentication key-chain

	Use this command to set the key-chain used by the IS-IS interface authentication. Use the no form of this command to cancel the specified key-chain.	
	isis authentication key-chain <i>name-of-chain</i> [level-1 level-2]	
	no isis authentication key-chain <i>name-of-chain</i> [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>name-of-chain</i>	Key-chain name with the maximum length being 255.
	level-1	Specifies the authentication key-chain of the Level-1.
	level-2	Specifies the authentication key-chain of the Level-2.
Defaults	By default, no IS-IS interface authentication key-chain is specified.	
Command Mode	Interface configuration mode	
Usage Guide	If the key chain command is not used to configure the corresponding key-chain, the authentication will not be performed. In addition, to make the IS-IS key-chain authentication effective, you need to configure the isis authentication mode command at the same time. This key-chain can apply to the plain-text authentication mode and MD5 encrypted authentication mode. You can use the isis authentication mode command to set the authentication mode. The length of the password key-string in the key-chain shall not be larger than 254 characters if the plain-text authentication mode is used, otherwise this configuration will fail. Only one key-chain is used at one time. So, when configuring this command, the said key-chain will be	

	overwritten by the new specified one. If the Level is not specified, the key-chain will apply to both Level-1 and Level-2. The key-chain specified by this command works on the Hello packets. The IS-IS will send or receive the password that belongs to this key-chain. There may contain multiple passwords in the key-chain. When sending the packets, use the password with small number first. While receiving the packets, the packet will be received as long as the password of this packet received corresponds to any password in the key-chain. The authentication commands configured in the IS-IS configuration mode such as authentication key-chain are effective to the LSP, SNP packets, but take no effect on the IS-IS interface.									
Configuration Examples	The following example specifies the authentication key-chain of the interface GigabitEthernet 0/1 named as <i>kc</i>. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis authentication key-chain kc</pre>									
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>isis authentication mode</td><td>Specifies the mode of IS-IS interface authentication.</td></tr><tr><td>isis authentication send-only</td><td>Specifies the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.</td></tr><tr><td>key-chain</td><td>Configures the key-chain.</td></tr></table>	Command	Description	isis authentication mode	Specifies the mode of IS-IS interface authentication.	isis authentication send-only	Specifies the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.	key-chain	Configures the key-chain.	
Command	Description									
isis authentication mode	Specifies the mode of IS-IS interface authentication.									
isis authentication send-only	Specifies the IS-IS interface authentication only applicable to the packets sent, but not to the packets received.									
key-chain	Configures the key-chain.									
Platform Description	N/A									

4.26 isis authentication mode

	Use this command to specify the mode of IS-IS interface authentication. Use the no form of this command to remove the configuration.	
	isis authentication mode { md5 text } [level-1 level-2]	
	no isis authentication mode { md5 text } [level-1 level-2]	
Parameter Description	Parameter	Description
	md5	Specifies the MD5 authentication mode.
	text	Specifies the plain-text authentication mode.
	level-1	Specifies the interface authentication mode to take effect on the Level-1.
	level-2	Specifies the interface authentication mode to take effect on the Level-2.
Defaults	By default, no interface authentication mode is specified.	
Command Mode	Interface configuration mode	

Usage Guide	To make the key-chain configured by the isis authentication key-chain command take effect, you must use the isis authentication mode command to specify the authentication mode. If the Level is not specified, the authentication mode specified will apply on both Level-1 and Level-2. When configuring the isis authentication mode command, if the isis password has been executed, the set command will be overwritten by this command. If the isis authentication mode command has been executed, the isis password will not be configured successfully. So, you need to delete the isis authentication mode command first.	
Configuration Examples	The following example specifies the authentication mode on the Level-2 of the interface GigabitEthernet 0/1 to be the MD5 authentication mode. FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis authentication mode md5 level-2	
Related Commands	Command	Description
	isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
	isis authentication send-only	Specifies the IS-IS interface authentication to only apply on the packets sent, but not on the packets received.
	key-chain	Configures the key-chain.
	isis password	Sets the plain-text authentication password for the packets transmit on the IS-IS interface.
Platform Description	N/A	

4.27 isis authentication send-only

	Use this command to specify the IS-IS interface authentication to only apply to the packets sent and not to the packets received. Use the no form of this command to restore the authentication of packets received on the interface.	
	isis authentication send-only [level-1 level-2]	
	no isis authentication send-only [level-1 level-2]	
Parameter Description	Parameter	Description
	level-1	Set the send-only on the Level-1 of the interface.
	level-2	Set the send-only on the Level-2 of the interface.
Defaults	By default, this command is not configured. If the IS-IS interface authentication has been configured, then the authentication will be performed on the packets sent and recieved at the same time.	
Command	Interface configuration mode	

Mode		
Usage Guide	With this command configured, the IS-IS will set the authentication password in the Hello packets sent from the interface, however, the authentication will not be performed on the Hello packets received. It can apply to the following two occasions: 1. before deploying the IS-IS interface authentication for all devices in the network. 2. before changing the authentication password or authentication mode. Before the above two tasks start, you need to configure the isis authentication send-only command first to make each device perform no authentication on the Hello packets received, so as to avoid the network oscillation caused during the subsequent IS-IS interface authentication deployment. After the deployment of the entire network authentication finished, execute the no isis authentication send-only command to cancel the send-only authentication mode. This command can apply to the plain-text authentication mode and MD5 authentication mode. You can use the isis authentication mode command to set the mode used by the IS-IS interface authentication. If the Level is not specified, the authentication mode specified is applicable to the Level-1 and Level-2.	
Configuration Examples	The following example specifies the authentication on the Level-1 of the interface GigabitEthernet 0/1 using send-only authentication mode. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis authentication send-only level-1</pre>	
Related Commands	Command	Description
	isis authentication key-chain	Specifies the key-chain used by the IS-IS interface authentication.
	isis authentication mode	Specifies the mode of the IS-IS interface authentication.
	key-chain	Configures the key-chain.
Platform Description	N/A	

4.28 isis bfd

	Use this command to enable association between IS-IS and BFD on an interface. isis bfd [disable anti-congestion]	
	Use the no form of this command to disable association between IS-IS and BFD on an interface. no isis bfd [disable anti-congestion]	
Parameter Description	Parameter	Description
	disable	Disables association between IS-IS and BFD on an interface.
	anti-congestion	Indicates the IS-IS BFD anti-flapping option.
Defaults	If the bfd all-interfaces command is configured, association between IS-IS and BFD is enabled on an interface.	

	If the bfd all-interfaces command is not configured, association between IS-IS and BFD is disabled on an interface.
	By default, the anti-flapping function is disabled.
Command Mode	Interface configuration mode
Default Level	14
Usage Guide	There are two methods for enabling or disabling association between IS-IS and BFD on interfaces. Method 1: In IS-IS routing process configuration mode, run the [no] bfd all-interfaces [anti-congestion] command to enable or disable association between IS-IS and BFD on all interfaces running the IS-IS protocol. Method 2: In interface configuration mode, run the isis bfd [disable anti-congestion] command to enable or disable association between IS-IS and BFD on a specified interface. In normal cases, the device with the BFD function enabled sends detection packets to detect the link status at an interval of several milliseconds. When a link exception such as link interruption occurs, the device with the BFD function enabled rapidly detects the link exception and informs a device running the IS-IS protocol to delete neighbors and delete neighbor availability information from LSP packets. The device running the IS-IS protocol performs route re-calculation and generates a new route, to bypass the failed link, thereby implementing fast convergence. With the introduction of some new technologies such as the Multi-Service Transport Platform (MSTP), link congestion easily occurs in peak hours. When congestion occurs, the device with the BFD function enabled rapidly detects a link exception, informs a device running the IS-IS protocol to delete a neighbor and delete neighbor availability information from LSP packets, and performs link switching to bypass the congested link. The interval for an IS-IS neighbor to send a Hello detection packet is 10 seconds, and the timeout time is 30 seconds. When an exception is detected via the BFD function, IS-IS Hello packets can be normally received, the IS-IS neighbor relationship can be rapidly reestablished, and the route is restored to pass the congested link. Then, BFD is performed again. If there is still a link exception, link switching is performed repeatedly. The route switches between the congested link and other links and flapping occurs. The anti-flapping function can be enabled to prevent route flapping in the case of link congestion. After the anti-flapping function is enabled, if a link is congested, the IS-IS neighbor keeps alive but the neighbor availability information in LSP packets is deleted, and the route switches to a non-congested link. After the link is restored, that is, congestion is eliminated, the neighbor availability information is restored in LSP packets, and the route switches back to the originally congested link, thereby preventing route flapping. When IS-IS anti-flapping is enabled, the BFD anti-flapping command (bfd up-dampening) must be configured on an interface. The two commands must be configured simultaneously. If only one of them is configured, the anti-flapping function does not take effect or a network exception is incurred.  Before association between IS-IS and BFD is configured, a BFD session must be configured on an interface.  When the BFD anti-flapping command is configured on an interface, if association between IS-IS and BFD is already configured on the interface, the anti-flapping function must be enabled for a device running the IS-IS protocol.

	 When the IS-IS anti-flapping option is configured, the BFD anti-flapping command must be configured on an interface.
Configuration Examples	1. The following example disables association between IS-IS and BFD on GigabitEthernet 0/1. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# no switchport FS(config-if)# isis bfd disable</pre>
	2. The following example enables the IS-IS BFD anti-flapping option and configures the BFD anti-flapping command on GigabitEthernet 0/1. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# no switchport FS(config-if)# isis bfd anti-congestion FS(config-if)# bfd up-dampening 60000</pre>

4.29 isis circuit-type

	Use this command to set the circuit-type for the IS-IS interface. Use the no form of this command to restore the default settings.	
	isis circuit-type { level-1 level-1-2 level-2-only }	
	no isis circuit-type	
Parameter Description	Parameter	Description
	level-1	Forms the Level-1 adjacency.
	level-2-only	Forms the Level-2 adjacency.
	level-1-2	Forms the Level-1-2 adjacency.
	external	Uses the interface as an external domain interface.
Defaults	By default, the circuit-type is Level-1-2.	
Command Mode	Interface configuration mode	
Usage Guide	If the circuit type is set to Level-1 or Level-2-only, IS-IS will only send PDUs of the corresponding Level. If the system type is set to Level-1 or Level-2-only, IS-IS only processes the instances of the corresponding Level, and the interface only sends the PDUs of the same Level specified by the is-type and circuit-type commands. If the interface is set to external, the interface will work as an external domain interface and IS-IS will not send PDUs of the corresponding Level.	
Configuration	FS(config)# interface GigabitEthernet 0/1	

Examples	FS(config-if)# isis circuit-type level-2-only	
Related Commands	Command	Description
	isis-type	Sets the Level of IS-IS instance.
Platform Description	N/A	

4.30 isis csnp-interval

	Use this command to set the interval for broadcasting the CSNP packets on the IS-IS interface, with the unit being second. Use the no form of this command to restore the default interval.	
	isis csnp-interval <i>interval</i> [level-1 level-2]	
	no isis csnp-interval [<i>interval</i>] [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>interval</i>	Interval for sending the CSNP packets in the range of 0 to 65535, with the unit being second.
	level-1	Interval for sending the CSNP packets configured only on the Level-1.
	level-2	Interval for sending the CSNP packets configured only on the Level-2.
Defaults	By default, in the broadcast network, the interval for sending the CSNP packets is 10 seconds. While in the P2P interface network, no CSNP packet is sent by default. When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.	
Command Mode	Interface configuration mode	
Usage Guide	Configure this command to change the interval for sending the CSNP packets. By default, the DIS on the broadcast network sends the CSNP packets every 10 seconds. For the P2P interface network, by default, the CSNP packets will only be sent at the beginning of adjacency formation. If the interface is set to mesh-groups, you can configure the periodic sending of the CSNP packets. If the csnp-interval is set to 0, no CSNP packets will be sent.	
Configuration Examples	FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis csnp-interval 20	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

4.31 isis hello-interval

	Use this command to set the interval for sending Hello packets on the interface, with the unit being second. Use the no form of this command to restore the default interval.	
	isis hello-interval { <i>interval</i> minimal } [level-1 level-2]	
	no isis hello-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>interval</i>	Interval for sending the Hello packet, in the range of 1 to 65536.
	minimal	The holdtime is set to the minimal value 1.
	level-1	This interval applies on the Level-1.
	level-2	This interval applies on the Level-2.
Defaults	By default, the interval value is 10 seconds, which is applicable to the Level-1 and Level-2 at the same time. When using this command without the parameter Level-1 and Level-2, the new setting is defaulted to be applicable to the Level-1 and Level-2 at the time.	
Command Mode	Interface configuration mode	
Usage Guide	Configure this command to change the interval for sending Hello packets. By default, the multiplier of the Hello holdtime is 3, and the DIS in broadcast network sends Hello packets at an interval which is three times of non-DIS. If this IS is elected as DIS on this interface, the interface will send Hello packets every 3.3 seconds by default. If the key word "minimal" is used, then the "holdtime" in Hello packets will be set to 1, and hello interval will be calculated based on the hello-multiplier. For example, if hello-multiplier is configured to 4 and "isis hello-interval minimal" is configured at the same time, the value of hello-interval shall be 1s/4 (250ms). By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example , the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the limit of IS-IS packets using the global commands cpu-protect type isis-is pps, cpu-protect type isis-l1is pps and cpu-protect type isis-l2is pps.	
Configuration Examples	The following example sets the interval for sending Hello packets on the interface.	
	<pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis hello-interval 5 level-1</pre>	
	The following example sets the Holdtime for sending Hello packets on the interface to the minimum value 1.	
	<pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis hello-interval minimal</pre>	

Related Commands	Command	Description
	isis hello-multiplier	Sets the multiplier of the Hello hold timer.
Platform Description	N/A	

4.32 isis hello-multiplier

	Use this command to set the multiplier of Hello hold timer. Use the no form of this command to restore the default settings.	
	isis hello-multiplier <i>multiplier-number</i> [level-1 level-2]	
	no isis hello-multiplier [<i>multiplier-number</i>] [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>multiplier-number</i>	Multiplier value in the range of 2 to 100.
Defaults	By default, the multiplier is 3..	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set the multiplier of Hello holdtime. The holdtime value in the Hello packet is the product of hello-interval and this multiplier.	
Configuration Examples	FS(config)# router isis FS(config-router)# isis hello-multiplier 5	
Related Commands	Command	Description
	isis hello-interval	Sets the interval for sending the Hello packets.
Platform Description	N/A	

4.33 isis hello padding

	Use this command to specify the filling mode for the IS-IS Hello packets. Use the no form of this command to fill no IS-IS Hello packets.	
	isis hello padding	
	no isis hello padding	

Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Interface configuration mode	
Usage Guide	Fill the IS-IS Hello packets to advertise the MTU supported to the neighbors. Hello packets can be padded to notify a neighbor of the MTU supported by the local device. In IS-IS routing process configuration mode, the corresponding hello padding command also exists. Hello packets sent by a specific interface are not padded if the padding of such Hello packets is cancelled in IS-IS routing process configuration mode or the padding of Hello packets sent by the local interface is cancelled in interface configuration mode.	
Configuration Examples	The following example fills no IS-IS Hello packets. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# no isis hello padding</pre>	
Related Commands	Command	Description
	isis hello-interval	Sets the interval for sending the Hello packets.
Platform Description	N/A	

4.34 isis lsp-interval

	Use this command to set the interval for the LSP PDU transmission. Use the no form of this command to restore the default interval.	
	isis lsp-interval <i>milliseconds</i> [level-1 level-2]	
	no isis lsp-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	milliseconds	Indicates the LSP interval. The value range is 1 to 4,294,967,295, in the unit of milliseconds.
	level-1	Applies the setting only to Level-1 LSPs.
	level-2	Applies the setting only to Level-2 LSPs.
Defaults	By default, the lsp-interval is 33ms.	
Command Mode	Interface configuration mode	

Usage Guide	N/A				
Configuration Examples	The following example sets the interval for the LSP PDU transmission to 100. FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis lsp-interval 100				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>isis retransmit-interval</td><td>Sets the LSP retransmission interval in the P2P network.</td></tr> </table>	Command	Description	isis retransmit-interval	Sets the LSP retransmission interval in the P2P network.
Command	Description				
isis retransmit-interval	Sets the LSP retransmission interval in the P2P network.				
Platform Description	N/A				

4.35 isis mesh-group

	Use this command to add the interface to the specified mesh-group. Use the no form of this command to separate the interface from the mesh-group.	
	isis mesh-group { blocked mesh-group-id }	
	no isis mesh-group	
Parameter Description	Parameter	Description
	blocked	Blocks all LSP forwarding on the interface.
	<i>mesh-group-id</i>	Adds the interface to the mesh-group of specified mesh-group-id with the range being 1 to 4,294,967,295.
Defaults	By default, the interface is not added to any mesh-group.	
Command Mode	Interface configuration mode	
Usage Guide	Mesh-groups can control the exceeding and redundant LSP spreading in the NBMA network. In the normal condition, the IS-IS router spreads out the LSP from all interfaces except for the receiving one, that is, if a router is configured multiple subinterfaces, the LSP will be sent from all subinterfaces and the neighbors will receive many same LSPs, which wastes a large number of CPU and bandwidth. The IS-IS mesh-group allows grouping the router interfaces, so if a LSP is received by one subinterface in the group, this LSP will not be spread out through other subinterfaces in the group. And if the router receives the LSP from the interface out of the group, it will spread out the LSP from other interfaces as usual. If you need to configure the mesh-group on the IS-IS interface, use the isis csnp-interval command to configure the interval for sending the non-0 CSNP packets, so as to send the CSNP packets regularly to synchronize the LSP and ensure the integrity of LSP synchronization between neighbors in network.	

Configuration Examples	FS#configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis mesh-group 1	
Related Commands	Command	Description
	isis network point-to-point	Sets the Broadcast interface type of IS-IS to Point-to-Point.
Platform Description	N/A	

4.36 isis metric

	Use this command to set the metric for the interface. Use the no form of this command to restore the default metric.	
	isis metric <i>metric</i> [level-1 level-2]	
	no isis metric [<i>metric</i>] [level-1 level-2]	
Parameter Description	Parameter	Description
	metric	Metric value in the range of 1 to 63.
	level-1	Sets this metric to apply on the Level-1 circuit.
	level-2	Sets this metric to apply on the Level-2 circuit.
Defaults	By default, the metric is 10, which applies on both Level-1 and Level-2 circuit.	
Command Mode	Interface configuration mode	
Usage Guide	The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF. This value is effective only when the metric-style includes narrow.	
Configuration Examples	FS(config)# interface GigabitEthernet 0/1 FS(config-if)#isis metric 1	
Related Commands	Command	Description
	metic-style	Sets the metric type.
	isis wide-metric	Sets the wide metric of the IS-IS interface.
Platform Description	N/A	

4.37 isis network point-to-point

	Use this command to set the IS-IS Broadcast interface to the Point-to-Point type. Use the no form of this command to restore the interface type to the Broadcast.	
	isis network point-to-point	
	no isis network point-to-point	
Parameter Description	Parameter	Description
	point-to-point	Point-to-Point type interface.
Defaults	By default, it is Broadcast type.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	<pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis network point-to-point</pre>	
Related Commands	Command	Description
	isis mesh-group	Adds the IS-IS interface into the specified mesh group.
Platform Description	N/A	

4.38 isis password

	Use this command to set the plain-text authentication password for the Hello packet transmitted on the interface. Use the no form of this command to remove the configurations.	
	isis password <i>password-string</i> [send-only] [level-1 level-2]	
	no isis password [send-only] [level-1 level-2]	
Parameter Description	Parameter	Description
	0	Indicates that the key is displayed in plaintext.
	7	Indicates that the key is displayed in ciphertext.
	password-string	Indicates the password string for plaintext authentication. The string can contain up to 126 characters.
	send-only	Indicates that the plaintext authentication password is only used to authenticate sent packets. Received packets are not authenticated.

	level-1	Applies the setting to the Level-1 circuit type.
	level-2	Applies the setting to the Level-2 circuit type.
Defaults	By default, both the passwords on the Level-1 and Level-2 are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to set the plain-text authentication password for the Hello packets transmitted on the interface. Use the no form of this command to clear the passwords. When the Level is not specified, the authentication password configured is by default applicable to every Level. If the isis authentication mode command has been executed, this command will not be configured successfully. To configure this command, you need to delete the isis authentication mode command first. Running the no isis password send-only command can only disable the send-only option.	
Configuration Examples	<pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis password redgiant</pre>	
Related Commands	Command	Description
	isis authentication mode	Specifies the mode of the IS-IS interface authentication.
Platform Description	N/A	

4.39 isis priority

	Use this command to set the priority for the DIS election on the LAN. Use the no form of this command to restore the default priority.	
	isis priority <i>value</i> [level-1 level-2]	
	no isis priority [<i>value</i>] [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>value</i>	Value of the priority in the range of 0 to 127.
	level-1	Applies to the Level-1 circuit.
	level-2	Applies to the Level-2 circuit.
Defaults	The default priority value is 64 and it is applied on both Level-1 and Level-2 circuit.	
Command Mode	Interface configuration mode	

Usage Guide	Use this command to change the priority value in the Hello of LAN. The low priority value has the lower priority in the DIS election than the high priority value. This command takes no effect on the Point-to-Point network interface. The no isis priority command is used to restore the priority to the default value no matter whether the parameter is followed. If you want to modify the configured priority, you can either use the isis priority command with parameter specified to overwrite the configured command directly, or configure a new parameter after restoring the priority to the default value.	
Configuration Examples	<pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis priority 127 level-1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.40 isis psnp-interval

	Use this command to set the minimum transmission interval of PSNP packets. isis psnp-interval <i>seconds</i> [level-1 level-2]	
	Use the no form of this command to cancel the specified minimum transmission interval of PSNP packets. no isis psnp-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	seconds	Indicates that the value range is 1 to 120 in seconds.
	level-1	Indicates that the configuration takes effect only at Level-1.
	level-2	Indicates that the configuration takes effect only at Level-2.
Defaults	This command is not configured by default. The default minimum transmission interval is 2 seconds and takes effect both at Level-1 and Level-2.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	PSNP packets are used to request for LSP packets or respond to received LSP packets in a point-to-point network. In both cases, it is recommended to send PSNP packets rapidly. If there are excessive LSP packets but the device performance is poor, you can set the PSNP packet transmission interval and LSP retransmission time to larger values,	

	to reduce the device load.
Configuration Examples	The following example sets the PSNP packet transmission interval to 5 seconds for Interface GigabitEthernet 0/1 at Level-2. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# isis psnp-interval 5 level-2</pre>

4.41 isis retransmit-interval

	Use this command to set the LSP retransmission interval. Use the no form of this command to restore the default interval.	
	isis retransmit-interval <i>seconds</i> [level-1 level-2]	
	no isis retransmit-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	seconds	Indicates the LSP retransmission interval. The value range is 0 to 65,535, in the unit of seconds.
	level-1	Applies the setting only to Level-1 LSPs.
	level-2	Applies the setting only to Level-2 LSPs.
Defaults	The default value is 5s.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to configure the LSP retransmission interval. In a P2P network, after a device sends an LSP, if the device receives no PSNP response within the time specified by this command, it will resend the LSP. If the retransmission interval is set to 0, the LSP will not be resent.	
	The following example sets the LSP retransmission interval to 10s.	
Configuration Examples	<pre>FS(config)# interface serial 0/1 FS(config-if)# isis retransmit-interval 10 level-2</pre>	
Related Commands	Command	Description
	isis lsp-interval	Configures the interval for LSP advertisement on the interface.
Platform Description	N/A	

4.42 isis subvlan

	Use this command to enable IS-IS on super VLANs. Use the no form of this command to restore the default setting.	
	isis subvlan [all vid]	
	no isis subvlan	
Parameter Description	Parameter	Description
	all	Indicates that packets are allowed to be sent to all sub VLANs.
	vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Defaults	The default setting takes effect only on super VLANs with IS-IS disabled.	
Command Mode	Interface configuration mode.	
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when IS-IS multicast packets are sent over a super VLAN containing multiple sub VLANs, the IS-IS multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the IS-IS function does not need to be enabled on a super VLAN. Therefore, the IS-IS function is disabled by default. However, in some scenarios, the IS-IS function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.	
Configuration Examples	The following example sends the IS-IS multicast packets to sub VLAN 1024 of super VLAN 300. <pre>FS(config)# interface vlan 300 FS(config-if-VLAN 300)# isis subvlan 1024</pre>	

4.43 isis three-way-handshake disable

	Use this command to disable three-way handshake for point-to-point network. Use the no form of this command to enable three-way handshake for point-to-point network.	
	isis three-way-handshake disable	
	no isis three-way-handshake disable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, three-way handshake is enabled.	

Command Mode	Interface configuration mode	
Usage Guide	In the point-to-point network, three-way handshake is enabled by default. That is to say, the IS-IS neighbor can be established only after three-way handshake is successful. You can use this command to cancel three-way handshake negotiation to accelerate IS-IS neighbor establishment or for the the device not supporting three-way handshake.	
Configuration Examples	The following example disables three-way handshake on interface GigabitEthernet 0/0. FS(config)#int GigabitEthernet 0/0 FS(config-if)# isis network point-to-point FS(config-if)# isis three-way-handshake disable	
Related Commands	Command	Description
	metric-type	Sets the metric type.
	isis metric	Sets the metric value of the interface.
Platform Description	N/A	

4.44 isis wide-metric

	Use this command to set the wide metric of the interface. Use the no form of this command to restore the default wide metric.	
	isis wide-metric <i>metric</i> [level-1 level-2]	
	no isis wide-metric [<i>metric</i>] [level-1 level-2]	
Parameter Description	Parameter	Description
	metric	Metric value in the range of 1 to 16,777,241.
	level-1	Sets this Metric to apply on the Level-1 circuit.
	level-2	Sets this Metric to apply on the Level-2 circuit.
Defaults	By default, the metric value is 10 and it is applicable to both Level-1, Level-2 circuit.	
Command Mode	Interface configuration mode	
Usage Guide	The Metric value is in the TLV of the IP reachable information and is applied to the SPF calculation. The greater metric value means the more routing cost on this interface and the longer path calculated by SPF. This value is effective only when the metric-style includes wide.	
Configuration	FS(config)# interface GigabitEthernet 0/1	

Examples	FS(config-if)# isis wide-metric 1000	
Related Commands	Command	Description
	metric-type	Sets the metric type.
	isis metric	Sets the metric value of the interface.
Platform Description	N/A	

4.45 is-type

	Use this command to specify the level for the IS-IS process. Use the no form of this command to restore the default level for IS-IS process.	
	is-type { level-1 level-1-2 level-2-only }	
	no is-type	
Parameter Description	Parameter	Description
	level-1	Specifies the IS-IS process running on the Level-1 only.
	level-1-2	Specifies the IS-IS process running on both Level-1 and Level-2.
	level-2-only	Specifies the IS-IS process running on the Level-2 only.
Defaults	By default, the IS-IS process runs on Level-1-2.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Changing the is-type enables or disables the route of one Level.	
Configuration Examples	FS(config)# router isis FS(config-router)# is-type level-1	
Related Commands	Command	Description
	isis circuit-type	Sets the type of Interface circuit.
Platform Description	N/A	

4.46 log-adjacency-changes

	Use this command to log the changes of the IS adjacency status in case of debug disabled. Use the no form of this command to disable this function.

	log- adjacency-changes	
	no log- adjacency-changes	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, this function is enabled.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	You can also use the debug command to log the changes of the IS adjacency status. But using the IS-IS debug command will exhaust large numbers of resources.	
Configuration Examples	FS(config)# router isis FS(config-router)# log-adjacency-changes	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.47 lsp-fragments-extend

	Use this command to enable the LSP fragment extension mode for a level. Use the no form of this command to disable the LSP fragment extension mode for a level.	
	lsp-fragments-extend [level-1 level-2] [compatible rfc3786]	
	no lsp-fragments-extend [level-1 level-2] [compatible rfc3786]	
Parameter Description	Parameter	Description
	level-1	Enables the LSP fragment extension mode for the Level-1 only.
	level-2	Enables the LSP fragment extension mode for the Level-2 only.
	compatible	Compatible with RFC3786
	rfc3786	The older version of extended LSP implementation.
Defaults	By default, LSP fragment extension is disabled. If no level is specified, the LSP fragment extension mode is enabled for both Level-1 and Level-2.	
Command Mode	IS-IS routing process configuration mode	

Usage Guide	The originating LSP can be divided up to 256 fragments. After the 256 fragments are filled, the subsequent link state information, such as the neighbor and IP routing, will be discarded, resulting in network problem. To avoid the above problem, you can enable the LSP fragment extension function, and configure the additional system ID using the virtual-system command. If there are other vendor’s device supporting RFC3786 standard in the network, you need to display the link state database of the device when enabling or disabling the compatible option. If there is indeed the vendor’s device, you can use the clear isis * command to clear the remaining LSP packets to trigger the system to update the link state database.	
Configuration Examples	The following example enables the LSP fragment extension mode for the Level-2. <pre>FS(config)# router isis FS(config-router)# lsp-fragments-extend level-2</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.48 lsp-gen-interval

	Use this command to set the minimal interval of the LSP generation. Use the no form of this command to restore the default value.	
	lsp-gen-interval [level-1 level-2] <i>maximum-interval</i> [<i>initial-interval</i> <i>hold-interval</i>]	
	no lsp-gen-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	level-1	Applies the configuration only to Level-1.
	level-2	Applies the configuration only to Level-2.
	<i>maximum-interval</i>	Indicates the maximum interval for generating two consecutive LSP packets. The value range is 1 to 65535 (in seconds). The default value is 5 .
	<i>initial-interval</i>	Indicates the waiting time for generating an LSP packet for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
	<i>hold-interval</i>	Indicates the minimum interval for generating an LSP packet for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .
Defaults	By default, this command is not configured and the interval of the minimal generation is 5s, it is effective on both Level-1 an Level-2	
Command	IS-IS routing process configuration mode	

Mode					
Usage Guide	The LSP packet generation interval refers to the interval for generating two different LSP packets. A smaller generation interval indicates faster network convergence, which, however, will be accompanied by frequent flooding on the network. The waiting time for generating an LSP packet for the first time is the initial interval. If the network becomes unstable, the LSP packet regeneration interval is changed to be less than the maximum interval, and the interval for generating an LSP packet for the second time becomes the hold interval. A corresponding penalty will be added to this interval: The next interval for regenerating a LSP packet doubles the previous interval for generating the same LSP packet, until the regeneration interval reaches the maximum interval. Subsequent LSP packets will be generated at the maximum interval. When the network becomes stable, the LSP packet regeneration interval becomes greater than the maximum interval, and the waiting time for LSP packet generation is restored to the initial interval. Link changes have high requirements for convergence. The initial interval can be set to a small value. The preceding parameters can also be adjusted to larger values to reduce CPU consumption. The value of initial-interval cannot be greater than that of maximum-interval. Otherwise, the value of initial-interval will be used as the value of maximum-interval. The value of hold-interval cannot be greater than that of maximum-interval. Otherwise, the value of hold-interval will be used as the value of maximum-interval. The value of initial-interval cannot be greater than that of hold-interval. Otherwise, the value of initial-interval will be used as the value of hold-interval.				
Configuration Examples	The following example sets the minimum interval for generating two duplicate LSP packets to 10 seconds, the interval for generating a duplicate LSP packet for the first time to 100 ms, and the interval for generating a duplicate LSP packet for the second time to 200 ms. <pre>FS(config)# router isis FS(config-router)# lsp-gen-interval 10 100 200</pre> The following example sets the minimum interval for generating two duplicate LSP packets to 5 seconds. <pre>FS(config)# router isis FS(config-router)# lsp-gen-interval 5</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>lsp-refresh-interval</td><td>Configures the interval for LSP refresh.</td></tr> </table>	Command	Description	lsp-refresh-interval	Configures the interval for LSP refresh.
Command	Description				
lsp-refresh-interval	Configures the interval for LSP refresh.				
Platform Description	N/A				

4.49 lsp-length originate

	Use this command to set the maximum length for transmitting LSP packets.
	lsp-length originate <i>size</i> [level-1 level-2]

	Use the no form of this command to restore the default value. no lsp-length originate [level-1 level-2]	
Parameter Description	Parameter	Description
	<i>size</i>	Specifies the maximum length for transmitting LSP packets. The value range is 512 to 16000 in bytes.
	level-1	Indicates that the configuration takes effect only at Level-1.
	level-2	Indicates that the configuration takes effect only at Level-2.
Defaults	The default value of the maximum length for transmitting LSP packets is 1492 . If no level is specified, the default value is level-1-2 , that is, the configuration takes effect at both Level-1 and Level-2.	
Command Mode	IS-IS routing process configuration mode	
Default Level	14	
Usage Guide	In principle, the length of LSP and SNP packets cannot be greater than the interface MTU. Otherwise, LSP packets and SNP packets are directly discarded upon being sent.	
Configuration Examples	The following example sets the maximum length for transmitting LSP packets at Level-2 to 1498 bytes. <pre>FS(config)# router isis 1 FS(config-router)# lsp-length originate 1498 level-2</pre>	

4.50 lsp-length receive

	Use this command to set the maximum length for receiving LSP packets. lsp-length receive size	
	Use the no form of this command to restore the default value. no lsp-length receive	
Parameter Description	Parameter	Description
	<i>size</i>	Specifies the maximum length of LSP packets. The value range is 1,492 to 16,000 in bytes according to the RFC.
Defaults	The default value is 1492 .	
Command Mode	IS-IS routing process configuration mode	
Default Level	14	

Usage Guide	This command is used to control the maximum length of LSP packets that can be received by the local device. In fact, to prevent a route convergence failure, intermediate nodes need to receive LSP packets with the maximum length of the interface MTU as long as the memory permits. In this sense, this command seems nominal. The maximum length for receiving LSP packets cannot be less than the maximum length for transmitting LSP packets. If the maximum length for receiving LSP packets is less than the maximum length for transmitting LSP packets, the maximum length for receiving LSP packets is automatically adjusted to the maximum length for transmitting LSP packets.
Configuration Examples	The following example configures the maximum length for receiving LSP packets to 1498 bytes. <pre>FS(config)# router isis FS(config-router)# lsp-length receive 1498</pre>

4.51 lsp-refresh-interval

	Use this command to set the LSP refresh interval. Use the no form of this command to restore the default value.	
	<code>lsp-refresh-interval interval</code>	
	<code>no lsp-refresh-interval</code>	
Parameter Description	Parameter	Description
	<i>interval</i>	LSP refresh interval in the range of 1 to 65535 with unit being second.
Defaults	By default, the <code>lsp-refresh-interval</code> is 900 seconds.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	If the LSP stable status lasts for the time of refresh interval, LSP will refresh this LSP and update the LSP version and publish it. It should be noted that the <code>lsp-refresh-interval</code> must be less than the max lifetime.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# lsp-refresh-interval 600</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.52 max-area-addresses

	Use this command to set the maximal number of area address allowed. Use the no form of this command to restore the default value.

	max-area-addresses <i>value</i>	
	no max-area-addresses	
Parameter Description	Parameter	Description
	<i>value</i>	The maximal number of area address allowed, in the range of 3 to 6.
Defaults	By default, the max-area-addresses is 3.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	For the IS routers of Level-1, only the ones with the same max-area-addresses are allowed to establish the adjacency relation.	
Configuration Examples	FS(config)# router isis FS(config-router)# max-area-addresses 5	
Related Commands	Command	Description
	net	Sets the IS-IS NET(Network Entry Title) address.
Platform Description	N/A	

4.53 maximum-paths

	Use this command to set the maximum number of IS-IS equal-cost routing entries in the routing table. maximum-paths <i>maximum</i>	
	Use the no form of this command to restore the default value. no maximum-paths	
Parameter Description	Parameter	Description
	<i>maximum</i>	Maximum number of IS-IS equal-cost routing entries in the routing table. The value range is 1 to device capacity .
Defaults	The default value is 2 .	
Command Mode	IS-IS routing process configuration mode, IS-IS address-family IPv6 configuration mode	
Default Level	14	

Usage Guide	This command is used by the IS-IS protocol to control the number of IS-IS equal-cost routing entries in the routing table. The routing table itself also has a command for controlling the number of equal-cost routing entries. The effective number of equal-cost routing entries is the smaller of the two values.
Configuration Examples	The following example sets the maximum number of IS-IS IPv4 equal-cost routing entries in the routing table to 5. <pre>FS(config)# router isis FS(config-router)# maximum-paths 5</pre> The following example sets the maximum number of IS-IS IPv6 equal-cost routing entries in the routing table to 6. <pre>FS(config)# router isis FS(config-router)# address-family ipv6 FS(config-router-af)# maximum-paths 6</pre>

4.54 max-lsp-lifetime

	Use this command to set the maximum value of the LSP lifetime. Use the no form of this command to restore the default value.	
	max-lsp-lifetime <i>value</i>	
	no max-lsp-lifetime	
Parameter Description	Parameter	Description
	<i>value</i>	Maximum value of the LSP lifetime in the range of 1 to 65,535, with unit being second.
Defaults	By default, the max-lsp-lifetime is 1200 seconds.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	It should be noted that the max-lsp-lifetime must be greater the lsp-refresh-interval 300.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# max-lsp-lifetime 1500</pre>	
Related Commands	Command	Description
	lsp-refresh-interval	Configures the interval for LSP refresh.
Platform Description	N/A	

4.55 metric-style

	Use this command to set the metric style. Use the no form of this command to restore the default metric style.	
	metric-style { narrow [transition] wide [transition] transition } [level-1 level-1-2 level-2]	
	no metric-style { narrow [transition] wide [transition] transition } [level-1 level-1-2 level-2]	
Parameter Description	Parameter	Description
	narrow	Uses the old metric style with the router interface metric ranging from 1 to 63.
	wide	Uses the new metric style with the router interface metric ranging from 1 to 16777214
	transition	Allows the router to send and receive the new and old metric style.
	level-1	This metric-style on the Level-1 circuit.
	level-2	This metric-style applies on the Level-2 circuit.
	level-1-2	This metric-style applies on the Level-1-2 circuit.
Defaults	By default, the metric-style is narrow.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	The metric value of the interface is specified by the isis metric <i>metric</i> when the metric-style is set to narrow, while the metric value is specified by the isis wide-metric <i>metric</i> in case that the metric-style is set to wide or transition .	
Configuration Examples	FS(config)# router isis FS(config-router)# metric-style wide	
Related Commands	Command	Description
	isis metric	Sets the metric of the interface.
	isis wide-metric	Sets the wide metric of the interface.
Platform Description	N/A	

4.56 multi-topology

	Use this command to enable IS-IS to support IPv6 unicast topology. Use the no form of this command to restore the default setting.
	multi-topology [transition]
	no multi-topology [transition]

Parameter Description	Parameter	Description
	transition	Configures the MT transition mode.
Defaults	By default, multitopology is not configured, namely, IS-IS does not support IPv6 unicast topology.	
Command Mode	IS-IS address-family IPv6 configuration mode	
Usage Guide	- When this command is not configured, IPv4 and IPv6 share the same IS-IS physical topology, which is also called default topology. - If the transition parameter is not specified, the device runs in multi-topology mode, the IS-IS v4 process works in the default topology while the IS-IS v6 process works in the IPv6 unicast topology. - If the transition parameter is specified, the device runs in multi-topology transition mode and the IS-IS v6 process runs in both the default topology and IPv6 unicast topology. The above three configurations are exclusive. The device which runs in multi-topology transition mode can transmit the multi-topology TLV and the default topology TLV. The multi-topology transition mode can be applied in incremental deployment to ensure smooth network migration. However, this mode may cause leaking of routes between the default topology and IPv6 unicast topology. Be careful to configure multi-topology transition mode, as this configuration may lead to network problems such as route blackhole and network loop. Before you configure this command, you need to set the metric style as wide or transition mode. Configuring the metric style as narrow and configuring only one Level to support wide or transition mode will disable the multitopology routing (MTR) function.	
Configuration Examples	The following example configures multi-topology. <pre>FS(config)# router isis FS(config-router)# address-family ipv6 FS(config-router-af)# multi-topology</pre>	
Related Commands	Command	Description
	router isis	Creates IS-IS instances.
Platform Description	N/A	

4.57 net

	Use this command to set the IS-IS NET (Network Entry Title) address. Use the no form of this command to delete this NET address.
	net <i>net-address</i>
	no net <i>net-address</i>

Parameter Description	Parameter	Description
	<i>net-address</i>	The format of net-address is shown as below: XX..XXXX.YYYY.YYYY.YYYY.00, the XX...XXXX is the area address and the YYYY.YYYY.YYYY is the system ID.
Defaults	By default, no NET address is set.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	This command is used to set the Area ID and System ID for the IS-IS. Up to three NET addresses are allowed to be set by default, namely three addresses with different Area can be set. However, the System ID must be the same.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# net 49.0000.0001.0002.0003.00</pre>	
Related Commands	Command	Description
	router isis	Creates IS-IS instances.
Platform Description	N/A	

4.58 passive-interface

	Use this command to configure the passive interface. Use the no form of this command to remove the passive interface.	
	passive-interface [default] { <i>interface-type</i> <i>interface-number</i> }	
	no passive-interface [default] { <i>interface-type</i> <i>interface-number</i> }	
Parameter Description	Parameter	Description
	default	Configures IS-IS disabled interfaces as passive.
	<i>interface-type</i>	Indicates the interface type.
	<i>interface-number</i>	Indicates the interface number.
Defaults	The passive interface is not configured by default.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Use this command to disable the interface to receive and send the IS-IS packets, but to advertise the IP address of	

	the interface. After the default option is configured, if the number of IS-IS disabled interfaces exceeds 255, the first 255 interfaces are configured as passive and the remaining interfaces are non-passive.	
Configuration Examples	The following example configures interface GigabitEthernet 0/0 as passive. FS(config)# router isis 1 FS(config-router)# passive-interface GigabitEthernet 0/0	
Related Commands	Command	Description
	router isis	Creates IS-IS instances.
Platform Description	N/A	

4.59 redistribute

	Use this command to redistribute the routes from one routing protocol into another routing protocol. Use the no form of this command to delete the redistribution.	
	redistribute { bgp ospf <i>process-id</i> match { internal external [1 2] nssa-external [1 2] } } rip connected static } [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-tag</i>] [level-1 level-1-2 level-2]	
	no redistribute { bgp ospf <i>process-id</i> [match { internal external [1 2] nssa-external [1 2] } } rip connected static } [metric <i>metric-value</i>] [metric-type { internal external }] [route-map <i>map-tag</i>] [level-1 level-1-2 level-2]	
Parameter Description	Parameter	Description
	<i>process-id</i>	OSPF process ID, in the range of 1 to 65535.
	match { internal external [1 2] nssa-external [1 2] }	Redistributes the OSPF routes to perform the filtering on the subtype of the OSPF routes. If the match option is not specified, all routes of the ospf subtype by default are received. If the 1 or 2 followed by the match external is not specified, then redistribute the route of the OSPF external1 and external 2 . if the 1 or 2 following the match nssa-external is not specified, then redistribute the routes of OSPF nssa-external 1 and nssa-external 2 .
	metric <i>metric-value</i>	Sets the metric value of redistributing the route, in the range of 0 to 4261412864. If the metric option is not specified, the external metric value is used.
	metric-type { internal external }	Sets the metric type of redistributing the route. internal : use the internal metric type. external : use the external metric type. If the metric-type is not specified, the internal type is used by default.
	route-map <i>map-tag</i>	Sets the route-map during the external routes redistribution, which is used to filter the redistributed routes or set attributions of the routes.

		The name of <i>map-tag</i> shall not be over 32 characters. No route-map is configured by default.
	level-1 level-1-2 level-2	Specifies the Level of receiving the redistributed routing information. If the Level is not specified, it is defaulted to be redistributed into the Level-2 . The format is shown as below: level-1: redistribute into the Level-1 level-1-2: redistribute into both Level-1 and Level-2. level-2: redistribute into the Level-2.
Defaults	By default, no redistribution is configured.	
Command Mode	IS-IS routing process configuration mode , IS-IS address-family ipv6 mode	
Usage Guide	Configure "no redistributbue { bgp ospf process-id rip connected static }" to disable protocol redistribution. If "no redistribute" is followed by any other parameter, it means that this parameter is restored to the default setting instead of disabling protocol redistribution. For example: "no redistribute bgp" will disable bgp redistribution, while "no redistribute bgp route-map aa" will disable route-map aa filtering during redistribution instead of disabling bgp redistribution. The routing information will be placed into the IP External Reachability Information TLV of LSP when redistributing external route in the IPv4 mode. The routing information will be placed to the IPv6 Reachable TLV of LSP when redistributing external route in the IPv6 mode. In the old version of some vendors, after configuring the metric-type to the external, the redistributed route metric will be added by 64 and then perform the routing according to the metric value during the routing calculation, which violates the protocol. In actual application, the priority of the external route may be higher than that of the internal route. When connecting with these old version of some vendors, the related configuration (such as the metric or the metric-type)of each device can be modified to ensure that the priority of the internal route is higher than the external.	
	The following example sets the metric value to 10.	
Configuration Examples	<pre>FS(config)# router isis FS(config-router)# redistribute ospf 1 metric 10 level-1</pre>	
Related Commands	Command	Description
	redistribute isis [tag] level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.
	redistribute isis [tag] level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.
	route-map	Configures the route map.
Platform Description	N/A	

4.60 redistribute isis level-1 into level-2

	Use this command to redistribute the Level-1 reachable routing information of the IS-IS instance into the Level-2 of current instance. Use the no form of this command to disable this redistribution.	
	redistribute isis [<i>tag</i>] level-1 into level-2 [route-map <i>route-map-name</i> distribute-list <i>access-list-name</i>]	
	no redistribute isis [<i>tag</i>] level-1 into level-2 [route-map <i>route-map-name</i> distribute-list <i>access-list-name</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	Name of the IS-IS instance.
	route-map <i>route-map-name</i>	Sets the route map during the route redistribution, which is used to filter the redistributed route and set attributions of this route. Name of the <i>route-map-name</i> shall not be over 32 characters. No route-map is configured by default.
	distribute-list <i>access-list-name</i>	Uses the distribute-list to filter the redistributed routes. Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below: {<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i> } In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i> .
Defaults	If the IS-IS Level-2 instance exists, all IS-IS Level-1 routes are by default redistributed into the IS-IS Level-2 instance.	
Command Mode	IS-IS routing process configuration mode or IS-IS address-family ipv6 mode.	
Usage Guide	Use the route-map or distribute-list to filter the Level-1 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.  You can only choose one of the two parameters route-map and distribute-list. Configure the no redistribute isis [<i>tag</i>] level-2 into level-1 to disable the specified instance redistribution. If the no redistribute is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution. For example: "no redistribute isis tag1 level-1 into level-2" will disable the isis tag1 redistribution, while "no redistribtue isis tag1 level-1 into level-2 route-map aa" will disable route-map aa filtering during redistribution instead of disabling the isis tag1 redistribution.	
Configuration Examples	<pre>FS(config)# router isis aa FS(config-router)# redistribute isis bb level-1 into level-2</pre>	
Related Commands	Command	Description
	redistribute	Redistributes the routing information from another routing protocol.

	redistribute isis level-2 into level-1	Redistributes the reachable routing information from Level-2 into Level-1.
Platform	N/A	
Description		

4.61 redistribute isis level-2 into level-1

	Use this command to redistribute the Level-2 reachable routing information of the IS-IS instance into the Level-1 of current instance. Use the no form of this command to remove the redistribution.	
	redistribute isis [<i>tag</i>] level-2 into level-1 [route-map <i>route-map-name</i> distribute-list <i>access-list-name</i> prefix <i>ip-address net-mask</i>]	
	no redistribute isis [<i>tag</i>] level-2 into level-1 [route-map <i>route-map-name</i> distribute-list <i>access-list-name</i> prefix <i>ip-address net-mask</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	Name of the IS-IS instance to be redistributed.
	route-map <i>route-map-name</i>	Sets the route map during the route redistribution, which is used to filter the redistributed routes and set attributions of the routes. Name of the <i>route-map-name</i> shall not be over 32 characters. No route-map is configured by default.
	distribute-list <i>access-list-name</i>	- Uses the distribute-list to filter the redistributed routes. - Access-list-name is the prefix list associated, it can be the standard, extended or naming prefix list. The format is shown as below: {<1-99> <100-199> <1300-1999> <2000-2699> <i>acl-name</i>} - In the IS-IS address-family ipv6 mode, you can use only the naming prefix list with the format being <i>acl-name</i>.
Defaults	N/A	
Command Mode	IS-IS routing process configuration mode or IS-IS address-family ipv6 mode.	
Usage Guide	Use the route-map or distribute-list to filter the Level-2 route of the specified instance to be redistributed. Only the route that meets the condition can be redistributed into the Level-1 of current instance.  You can only choose one of the two parameters route-map and distribute-list. Configure the no redistribute isis [<i>tag</i>] level-2 into level-1 to disable the specified instance redistribution. If the no redistribute is followed by any other parameters, it means that this parameter is restored to the default setting instead of disabling the specified instance redistribution. For example: "no redistribute isis tag1 level-2 into level-1" will disable the isis <i>tag1</i> redistribution, while "no redistribtue isis tag1 level-2 into level-1 route-map a" will disable route-map aa filtering during redistribution instead of disabling the isis <i>tag1</i> redistribution.	

Configuration	FS(config)# router isis <i>aa</i>	
Examples	FS(config-router)# redistribute isis <i>bb</i> level-2 into level-1	
Related Commands	Command	Description
	redistribute	Redistributes the routing information from another routing protocol.
	redistribute isis level-1 into level-2	Redistributes the reachable routing information from Level-1 into Level-2.
Platform Description	N/A	

4.62 router isis

	Use this command to create the IS-IS instance. Use the no form of this command to delete this instance.	
	router isis [<i>tag</i>]	
	no router isis [<i>tag</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	Instance name
Defaults	By default, no IS-IS instance is configured.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to initialize the IS-IS instance and enter the IS-IS routing process configuration mode. The IS-IS instance will not be executed unless one NET address is configured at least. When enabling the IS-IS routing process with the parameter <i>tag</i>, the parameter <i>tag</i> will be used as well when disabling the IS-IS routing process. By default, the CPU protection is enabled on the switch, so that the number of packets corresponding to the destination group addresses of ISIS (AllISSystems, AllL1ISSystems, AllL2ISSystems) is limited when they are sent to the CPU, for example , the default limited value is 400pps. The number of packets received by the switch may be larger than the default value if there are many neighbors or the interval for sending Hello packets is short, resulting in continual vibration of the adjacent relation. In this case, you need to raise the limit of IS-IS packets using the global commands cpu-protect type isis-is pps, cpu-protect type isis-l1is pps and cpu-protect type isis-l2is pps.	
Configuration Examples	FS# configure terminal FS(config)# router isis	

Related Commands	Command	Description
	ip router isis	Enables the IS-IS IPv4 routing protocol on the interface.
	ipv6 router isis	Enables the IS-IS IPv6 routing protocol on the interface.
	net	Sets the NET address.
Platform Description	N/A	

4.63 set-overload-bit

	Use this command to instruct a neighbor not to use the local IS-IS node as a transit device for forwarding data. set-overload-bit [on-startup <i>seconds</i>] [suppress { [interlevel] [external] }] [level-1 level-2]	
	Use the no form of this command to disable the function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data. no set-overload-bit [level-1 level-2]	
Parameter Description	Parameter	Description
	on-startup <i>seconds</i>	Indicates that an IS-IS node automatically enters the OVERLOAD state after restart. seconds is the duration of the IS-IS node in the OVERLOAD state after restart. The value range is 5 to 86,400 in seconds.
	suppress	Indicates that internal routes (IS-IS inter-area routes and intra-area routes) or external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state.
	interlevel	Indicates that IS-IS inter-area routes and intra-area routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
	external	Indicates that external routes are not advertised to neighbors when the IS-IS node is in the OVERLOAD state. It is used in combination with the suppress keyword.
	level-1	Sends LSP packets that carry the OVERLOAD bit only to Level-1 neighbors.
	level-2	Sends LSP packets that carry the OVERLOAD bit only to Level-2 neighbors.
Defaults	The function of instructing a neighbor not to use the local IS-IS node as a transit device for forwarding data is disabled by default.	
Command Mode	IS-IS routing process configuration mode	
Default Level	14	

Usage Guide	This command forces a IS-IS node to set the OVERLOAD bit in non-virtual LSP packets, to instruct IS-IS neighbors not to use the local node as a transit device. If the on-startup keyword is carried, the device automatically enters the OVERLOAD state after restart. If the on-startup keyword is not carried, the device immediately enters the OVERLOAD state upon restart.  The on-startup keyword takes effect for only one level. The OVERLOAD bit is mainly used in the following cases: ● Device overload The overload of the local IS-IS node, for example, memory insufficiency or CPU full load, may cause incomplete routes in the local routing table or no resource for data forwarding. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device. In this case, the on-startup keyword is not carried in the configuration. The OVERLOAD bit is manually set or cancelled. You must manually cancel this command after the local IS-IS node restores to the normal state. Otherwise, the local IS-IS node is always in the OVERLOAD state ● Instantaneous black hole In the scenario described in RFC3277, the IS-IS converges faster than BGP does. After an IS-IS node restarts, the route fails instantaneously, that is, instantaneous black hole occurs. You can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local node as a transit device till the specified timer expires. In this case, the configuration must carry the on-startup field. The OVERLOAD bit is automatically set or cancelled by the IS-IS node based on the configuration. After the on-startup field is selected, the IS-IS node automatically enters the instantaneous black hole state after restart. After a new neighbor relationship is established, the IS-IS node immediately sends the LSP packet that carries the OVERLOAD bit to notify the neighbor that the local device enters the instantaneous black hole state (or OVERLOAD state) and that the local node cannot be used as a transit device. When the specified timer expires, the IS-IS node immediately sends the LSP packet without the OVERLOAD bit to notify the neighbor that the local device is no longer in the instantaneous state (or OVERLOAD state) and can be used as a transit device. The timer time needs to be set based on the number of routes in the network. If there are many routes, set it to a large value; if there are a few routes, set it to a small value. ● The local IS-IS node is not intended to be used for forwarding real data If the local IS-IS node needs to be connected to the production network for testing or other function requirements and it is not intended to be used for forwarding real data in the network, you can set the OVERLOAD bit in LSP packets to instruct neighbors not to use the local device as a transit device. In this case, the on-startup field is not carried in the configuration and the OVERLOAD bit is manually set or cancelled. You can configure suppress as required to restrict the routing information carried in LSP packets in the OVERLOAD state, for example, suppress internal routes and external routes and advertise only local direct routes.
Configuration Examples	The following example sets an IS-IS node to immediately enter the instantaneous black hole state after restart till the specified timer expires (set the specified waiting time to 300 seconds) and advertises only local direct routes to neighbors. <pre>FS(config)# router isis</pre>

	FS(config-router)#set-overload-bit on-startup 300 suppress interlevel external
	The following example connects the local IS-IS node to the production network as a test device and set its not to forward real data of the production network, to avoid impact on production. <pre>FS(config)# router isis FS(config-router)#set-overload-bit suppress interlevel external</pre>

4.64 spf-interval

	Use this command to set the minimal interval for the SPF calculation. Use the no form of this command to restore the default minimal interval.	
	spf-interval [level-1 level-2] <i>maximum-interval</i> [<i>initial-interval</i> <i>hold-interval</i>]	
	no spf-interval [level-1 level-2]	
Parameter Description	Parameter	Description
	level-1	Applies the configuration only to Level-1.
	level-2	Applies the configuration only to Level-2.
	<i>maximum-interval</i>	Indicates the maximum interval for performing two consecutive SPF calculations. The value range is 1 to 120 (in seconds). The default value is 10 .
	<i>initial-interval</i>	Indicates the waiting time for performing the SPF calculation for the first time. The value range is 0 to 60000 (in milliseconds). The default value is 50 .
	<i>hold-interval</i>	Indicates the minimum interval for performing the SPF calculation for the second time. The value range is 10 to 60000 (in milliseconds). The default value is 200 .
Defaults	By default, this command is not configured. The default SPF interval is 10 seconds, which takes effect at both Level-1 and Level-2.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Increasing the maximum interval for performing SPF calculations can avoid frequent SPF calculations and waste of CPU resources. However, a larger minimum interval also leads to slower responses to route changes. The waiting time for performing the SPF calculation for the first time is the initial interval. If the network becomes unstable, the SPF calculation interval is less than the maximum interval, and the interval for performing the SPF calculation for the second time becomes the hold interval. A corresponding penalty is added to this interval: The next interval for the SPF calculation doubles the previous interval for the same SPF calculation, until the SPF calculation interval reaches the maximum interval. Subsequent SPF calculations are performed at the maximum interval. When the network becomes stable, the interval for performing the SPF calculation becomes greater than the maximum interval, and the waiting time for performing the SPF calculation is restored to the initial interval. Link changes have high requirements for convergence. The initial interval can be set to a small value. The preceding parameters can also be adjusted to larger values to reduce CPU consumption. The value of initial-interval cannot be greater than that of maximum-interval. Otherwise, the value of	

	initial-interval will be used as the value of maximum-interval. The value of hold-interval cannot be greater than that of maximum-interval. Otherwise, the value of hold-interval will be used as the value of maximum-interval. The value of initial-interval cannot be greater than that of hold-interval. Otherwise, the value of initial-interval will be used as the value of hold-interval.	
Configuration Examples	The following example sets the maximum interval for generating two duplicate SPF packets to 5 seconds, the interval for generating a duplicate SPF packet for the first time to 100 ms, and the interval for generating a duplicate SPF packet for the second time to 200 ms.	
	<pre>FS(config)# router isis FS(config-router)# spf-interval 5 100 200</pre>	
	The following example sets the maximum interval for generating two duplicate SPF packets to 10 seconds.	
	<pre>FS(config)# router isis FS(config-router)# spf-interval 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.65 summary-address

	Use this command to configure the IPv4 aggregation route. Use the no form of this command to delete the aggregation route.	
	summary-address <i>ip-address net-mask</i> [level-1 level-2 level-1-2] [metric <i>number</i>]	
	no summary-address <i>ip-address net-mask</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Indicates the IP address of the summary route.
	<i>net-mask</i>	Indicates the subnet mask of the summary route.
	level-1	Applies the setting only to Level-1.
	level-2	Applies the setting only to Level-2. By default, the setting takes effect for Level-2.
	level-1-2	Applies the setting to Level-1 and Level-2.
	<i>number</i>	Indicates the metric of the summary route.
Defaults	By default, no aggregation route is configured.	
Command Mode	IS-IS routing process configuration mode	

Usage Guide	With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.	
Configuration Examples	FS(config)# router isis FS(config-router)# summary-address 10.10.0.0/24 level-1-2	
Related Commands	Command	Description
	summary-prefix	Configures the IPv6 aggregation route.
Platform Description	N/A	

4.66 summary-prefix

	Use this command to configure the IPv6 aggregation route. Use the no form of this command to delete the aggregation route.	
	summary-prefix <i>ipv6-prefix/prefix-length</i> [level-1 level-2 level-1-2]	
	no summary-address <i>ipv6-prefix/prefix-length</i>	
Parameter Description	Parameter	Description
	ipv6-prefix / prefix-length	Aggregation network address and the IP prefix length of the aggregation network address.
	level-1	Applies to the Level-1 only.
	level-2	Applies to the Level-2 only.
	level-1-2	Applies to both Level-1 and Level-2.
Defaults	By default, no aggregation route is configured.	
Command Mode	Address-family ipv6 mode	
Usage Guide	With the aggregation route configured, if there is any reachable address or reachable network segment route in the aggregation route, it will publish the aggregation route instead of the detailed route.	
Configuration Examples	FS(config)# router isis FS(config-router)# address-family ipv6 FS (config-router-af)# summary-prefix 1000::/96 level-1-2	
Related Commands	Command	Description
	summary-address	Configures the IPv4 aggregation route.

Platform	N/A
Description	

4.67 two-way-maintain

	Use this command to enable the IS-IS two-way maintenance function. two-way-maintain	
	Use the no form of this command to disable the IS-IS two-way maintenance function. no two-way-maintain	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The IS-IS two-way maintenance function is enabled by default.	
Command Mode	IS-IS routing process configuration mode	
Default Level	14	
Usage Guide	In a large-scale network, a large number of packets are sent and received, which occupies lots of CPU and memory resources, causing the delay or discarding of some IS-IS packets. If the time required for processing hello packets exceeds the neighbor relationship maintenance duration, the corresponding neighbor relationship times out and is removed. When the two-way maintenance function is enabled, if a large number of packets exist on the network, the LSP packets, CSNP packets, and PSNP packets from a neighbor in addition to hello packets can also be used to maintain the two-way relationship with the neighbor, preventing the neighbor failure caused by delay or discarding of hello packets.	
Configuration Examples	The following example disables the IS-IS two-way maintenance function. FS(config)# router isis 1 FS(config-router)# no two-way-maintain	

4.68 virtual-system

	Use this command to configure an additional system ID for fragment extension. Use the no form of this command to remove the additional system ID.	
	virtual-system <i>system-id</i>	
	no virtual-system <i>system-id</i>	
Parameter Description	Parameter	Description
	<i>system-id</i>	Additional system ID. The length is 6 bytes.

Defaults	No additional system ID is configured by default.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Use this command to configure an additional system ID for LSP fragment extension. The system must be enabled with fragment extension mode and configured with the additional system ID to enable LSP fragment extension.	
Configuration Examples	The following example configures an additional system ID for fragment extension. <pre>FS(config)# router isis FS(config-router)# virtual-system 0000.0000.0034</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.69 vrf

	Use this command to bind the ISIS process with a VRF instance. Use the no form of this command to unbind the IS-IS process from the VRF instance.	
	vrf <i>vrf-name</i>	
	no vrf <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF instance name. The VRF instance must be configured.
Defaults	No IS-IS process is bound with the VRF instance.	
Command Mode	IS-IS routing process configuration mode	
Usage Guide	Before you configure this command, the specified VRF instance must be configured. If you want to build the IS-IS v6 neighbor, the multi-protocol VRF and IPv6 protocol must be enabled. The following restrictions are for binding IS-IS process with VRF instance: 1. The IS-IS process in the same non-default VRF instance must be configured with a different system ID. The IS-IS process in the different VRF instance can be configured with the same system ID. 2. An IS-IS process can be bound with only one VRF instance. A VRF instance can be bound with multiple IS-IS processes. 3. If a VRF instance bound with an IS-IS changes, the IS-IS enabled interfaces which are bound with the VRF	

	instance and the redistribute configuration in IS-IS routing process configuration mode will be removed.	
Configuration Examples	The following example binds an IS-IS process with a VRF instance. <pre>FS(config)#vrf definition vrf_1 FS(config-vrf)#address-family ipv4 FS(config-vrf-af)#exit-address-family FS(config)# router isis FS(config-router)# vrf vrf_1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.70 show clns is-neighbors

	Use this command to display all IS neighbors to provide the adjacency relationship of routers.	
	show clns [<i>tag</i>] is-neighbors [<i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
	<i>interface-type interface-number</i>	Specifies the name of interface.
	detail	Displays detailed information of all interfaces.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The output results of the show clns is-neighbors detail command are displayed as below: <pre> Area (null): System Id Type IP Address State Holdtime Circuit Interface r1 L1 1.0.0.2 Up 9 r1.01 GigabitEthernet 0/0 L2 1.0.0.2 Up 9 r1.01 GigabitEthernet 0/0 Adjacency ID: 1 Uptime: 00:00:54 Area Address(es): 49.1111 SNPA: 00d0.f8bc.de08 IPv6 Address(es): fe80::2a9:15ff:fe36:5413 Level-1 MTID: Standard Level-2 MTID: Standard Level-1 Protocols Supported: IPv4 Level-2 Protocols Supported: IPv4 </pre>	
Related Commands	Command	Description
	show clns neighbors	Displays all IS neighbors to provide the router information and the adjacency relationship of terminal system.
Platform Description	N/A	

4.71 show clns neighbors

	Use this command to display all IS neighbors to provide the router information and the adjacency relationship of terminal system.	
	show clns [<i>tag</i>] neighbors [<i>interface-type interface-number</i>] [detail]	
Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
	<i>interface-type interface-number</i>	Specifies the name of the interface.
	detail	Displays detailed information of all interfaces.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays all IS neighbors to provide the router information and the adjacency relationship of terminal system. <pre> FS# show clns neighbors detail Area (null): System Id SNPA State Holdtime Type Protocol Interface r1 00d0.f8bc.de08 Up 7 L1 IS-IS GigabitEthernet 0/0 Up 9 L2 IS-IS GigabitEthernet 0/0 Adjacency ID: 1 Uptime: 00:01:40 Area Address(es): 49.1111 IP Address(es): 1.0.0.2 IPv6 Address(es): fe80::2a9:15ff:fe36:5413 Level-1 MTID: Standard Level-2 MTID: Standard Level-1 Protocols Supported: IPv4, IPv6 Level-2 Protocols Supported: IPv4, IPv6 BFD(IPv4) session state: Up BFD(IPv6) session state: Up </pre>	
Related Commands	Command	Description
	show clns is-neighbors	Displays all IS neighbors to provide the router adjacency relationship.

Platform	N/A
Description	

4.72 show isis counter

	Use this command to display various statistics of IS-IS.	
	show isis [tag] counter	
Parameter Description	Parameter	Description
	tag	Specifies the IS-IS instance.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The output results of the show clns neighbors details are displayed as below: <pre> FS# show isis counter Area (null): IS-IS Level-1 isisSystemCounterEntry: isisSysStatCorrLSPs: 0 isisSysStatAuthTypeFails: 0 isisSysStatAuthFails: 0 isisSysStatLSPDbaseOloads: 0 isisSysStatManAddrDropFromAreas: 0 isisSysStatAttmpToExMaxSeqNums: 0 isisSysStatSeqNumSkips: 0 isisSysStatOwnLSPPurges: 0 isisSysStatIDFieldLenMismatches: 0 isisSysStatMaxAreaAddrMismatches: 0 isisSysStatPartChanges: 0 isisSysStatSPFRuns: 30 IS-IS Level-2 isisSystemCounterEntry: isisSysStatCorrLSPs: 0 isisSysStatAuthTypeFails: 0 isisSysStatAuthFails: 0 isisSysStatLSPDbaseOloads: 0 isisSysStatManAddrDropFromAreas: 0 isisSysStatAttmpToExMaxSeqNums: 0 isisSysStatSeqNumSkips: 0 isisSysStatOwnLSPPurges: 0 </pre>	

	isisSysStatIDFieldLenMismatches: 0 isisSysStatMaxAreaAddrMismatches: 0 isisSysStatPartChanges: 0 isisSysStatSPFRuns: 30	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.73 show isis database

	Use this command to display the LSP database.	
	show isis [<i>tag</i>] database [<i>FLAGS</i> <i>LEVEL</i> <i>LSPID</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
	<i>FLAGS</i>	The format is displayed as below: detail verbose detail: detailed information Verbose: more detailed information than the detail.
	<i>LEVEL</i>	The format is displayed as below: I1 I2 level-1 level-2 I1 and level-1: specify the LSP database of the Level-1. I2 and level-2: specify the LSP database of the Level-2
	<i>LSPID</i>	Specifies the ID number of LSP to show the corresponding LSP information only.
	<i>tag</i>	Specifies the IS-IS instance.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The output results of the show isis database detail command are displayed as below: FS# show isis database detail Area (null): IS-IS Level-1 Link State Database: LSPID LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL	


```

FS.00-00 * 0x00000007 0xCDD5          1011          0/0/0
  Area Address: 49.1111
  NLPID:      0xCC
  Hostname:   FS
  IP Address: 1.0.0.1
  Metric:    10      IS r1.01
  Metric:    10      IP 1.0.0.0 255.255.255.0
r1.00-00      0x00000006 0xA771          1032          0/0/0
  Area Address: 49.1111
  NLPID:      0xCC
  Hostname:   r1
  IP Address: 1.0.0.2
  Metric:    10      IS r1.01
  Metric:    10      IP 1.0.0.0 255.255.255.0
r1.01-00      0x00000002 0x062A          989           0/0/0
  Metric:     0      IS r1.00
  Metric:     0      IS FS.00

IS-IS Level-2 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
FS.00-00 * 0x0000000A 0xC7D8          1033          0/0/0
  Area Address: 49.1111
  NLPID:      0xCC
  Hostname:   FS
  IP Address: 1.0.0.1
  Metric:    10      IS r1.01
  Metric:    10      IP 1.0.0.0 255.255.255.0
r1.00-00      0x00000006 0xA771          1032          0/0/0
  Area Address: 49.1111
  NLPID:      0xCC
  Hostname:   r1
  IP Address: 1.0.0.2
  Metric:    10      IS r1.01
  Metric:    10      IP 1.0.0.0 255.255.255.0
r1.01-00      0x00000002 0x062A          989           0/0/0
  Metric:     0      IS r1.00
  Metric:     0      IS FS.00

```

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.74 show isis graceful-restart

	Use this command to display the status information related to the IS-IS GR.	
	show isis [tag] graceful-restart	
Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance name
Defaults	N/A	
Command Mode	Privileged EXEC mode/ global configuration mode/ interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the GR information of the IS-IS. <pre>FS(config)# show isis graceful-restart</pre> Area (null): Graceful-restart Helper: enabled Level 1: GigabitEthernet 0/0: RR received: 0 Level 2: GigabitEthernet 0/0: RR received: 0 Graceful-restart: enabled Graceful-period: 400s, Level timer: 60s, Interface timer: 3s Instance GR status: not restarting	
Related Commands	Command	Description
	graceful-restart	Enables the IS-IS GR Restart capability.
	graceful-restart grace-period	Configures the maximum interval of the grace-restart.
	graceful-restart helper disable	Disables the IS-IS GR Help capability.
	graceful-restart	Enables the IS-IS GR Restart capability.
Platform Description	N/A	

4.75 show isis hostname

	Use this command to display the mapping relation between the router name and system ID.
	show isis [tag] hostname

Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
Defaults	N/A	
Command Mode	Privileged EXEC mode/ global configuration mode/ interface configuration mode	
Usage Guide	N/A	
Configuration Examples	<pre> FS# show isis hostname System ID Dynamic Hostname Area (null) * 5555.5555.5555 FS 1111.1111.1111 R1 System ID Dynamic Hostname Area 1 * 4444.4444.4444 FS 2222.2222.2222 R2 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.76 show isis ipv6 topology

	Use this command to display information about the IPv6 unicast topology to which an IS-IS router is connected. show isis [<i>tag</i>] ipv6 topology [<i>I1</i> <i>I2</i> <i>level-1</i> <i>level-2</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	IS-IS instance
	I1	Topology of a specified Level-1 router
	level-1	Topology of a specified Level-1 router
	I2	Topology of a specified Level-2 router
	level-2	Topology of a specified Level-2 router
Command	Privileged EXEC mode, global configuration mode, and interface configuration mode	

Mode															
Default Level	14														
Usage Guide	N/A														
Configuration Examples	The following example displays the IPv6 unicast topology information. <pre>FS#show isis ipv6 topology Area (null): IS-IS paths to level-1 routers System Id Metric Next-Hop SNPA Interface r1 10 r1 00d0.f822.33ad GigabitEthernet 0/0 FS -- IS-IS paths to level-2 routers System Id Metric Next-Hop SNPA Interface r1 10 r1 00d0.f822.33ad GigabitEthernet 0/0 FS --</pre> Field description: <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>Area</td><td>Instance tag</td></tr> <tr> <td>System Id</td><td>System ID</td></tr> <tr> <td>Metric</td><td>Metric value</td></tr> <tr> <td>Next-Hop</td><td>Next hop</td></tr> <tr> <td>SNPA</td><td>SNPA address</td></tr> <tr> <td>Interface</td><td>Interface name</td></tr> </table>	Field	Description	Area	Instance tag	System Id	System ID	Metric	Metric value	Next-Hop	Next hop	SNPA	SNPA address	Interface	Interface name
Field	Description														
Area	Instance tag														
System Id	System ID														
Metric	Metric value														
Next-Hop	Next hop														
SNPA	SNPA address														
Interface	Interface name														

4.77 show isis interface

	Use this command to display the information about IS-IS interface.	
	show isis [<i>tag</i>] interface [<i>interface-type interface-number</i>] [<i>counter</i>]	
Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance name.
	<i>interface-type interface-number</i>	Specifies the Interface name.
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example displays the IS-IS interface. <pre>FS# show isis interface Area (null):</pre>	

	<pre> VLAN 1 is up, line protocol is up Routing Protocol: IS-IS ((null)) Network Type: Broadcast Circuit Type: level-1-2 Local circuit ID: 0x01 Extended Local circuit ID: 0x00000001 Local SNPA: 00d0.f822.33ab IP interface address: 1.0.0.1/24 Level-1 Metric: 10/10, Priority: 64, Circuit ID: r1.01 Level-1 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s, Retransmit:5s Level-1 LSPs in queue: 0 Level-1 LSPs flood: 5 Number of active level-1 adjacencies: 1 Level-2 Metric: 10/10, Priority: 64, Circuit ID: r1.01 Level-2 Timer intervals configured, Hello: 10s, Lsp: 33ms, Psnp: 2s, Csnp:10s, Retransmit:5s Level-2 LSPs in queue: 0 Level-2 LSPs flood: 5 Number of active level-2 adjacencies: 1 Next IS-IS LAN Level-1 Hello in 5 seconds Next IS-IS LAN Level-2 Hello in 5 seconds BFD Enabled (Anti-congestion) Eligible to backup traffic </pre>
	The following example displays the statistics of the IS-IS interface.
	<pre> FS# show isis interface counter Area (null): GigabitEthernet 1/1/0: IS-IS LAN Level-1 isisCircuitCounterEntry: isisCircAdjChanges: 4 isisCircNumAdj: 2 isisCircInitFails: 0 isisCircRejAdjs: 0 isisCircIDFieldLenMismatches: 0 isisCircMaxAreaAddrMismatches: 0 isisCircAuthTypeFails: 0 isisCircAuthFails: 0 isisCircLanDesISChanges: 1 IS-IS LAN Level-2 isisCircuitCounterEntry: </pre>

	<pre> isisCircAdjChanges: 4 isisCircNumAdj: 2 isisCircInitFails: 0 isisCircRejAdjs: 0 isisCircIDFieldLenMismatches: 0 isisCircMaxAreaAddrMismatches: 0 isisCircAuthTypeFails: 0 isisCircAuthFails: 0 isisCircLanDesISChanges: 1 IS-IS Level-1 isisPacketCounterEntry: isisPacketCountIIHello in/out: 187/278 isisPacketCountLSP in/out: 10/7 isisPacketCountCSNP in/out: 0/92 isisPacketCountPSNP in/out: 0/0 isisPacketCountUnknown in/out: 0/0 IS-IS Level-2 isisPacketCounterEntry: isisPacketCountIIHello in/out: 186/286 isisPacketCountLSP in/out: 17/9 isisPacketCountCSNP in/out: 1/91 isisPacketCountPSNP in/out: 0/0 isisPacketCountUnknown in/out: 0/0 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.78 show isis mesh-groups

	Use this command to display the mesh-group configurations on each interface.	
	show isis [tag] mesh-groups	
Parameter Description	Parameter	Description
	<i>tag</i>	Specifies the IS-IS instance.
Defaults	N/A	
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.	
	N/A	
Usage Guide		

Configuration Examples	The following example displays the mesh groups. FS# show isis mesh-groups Mesh group (blocked) FastEthernet 1/1 Mesh group 1 : FastEthernet 1/0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.79 show isis neighbors

	Use this command to display the IS-IS neighbors..																										
	show isis [<i>tag</i>] neighbors [<i>detail</i>]																										
Parameter Description	Parameter			Description																							
	<i>tag</i>			Displays the IS-IS instance.																							
	<i>detail</i>			Displays the detailed information of all interfaces.																							
Defaults	N/A																										
Command Mode	Privileged EXEC mode, global configuration mode or interface configuration mode.																										
Usage Guide	N/A																										
Configuration Examples	The following example displays details of IS-IS neighbors. FS# show isis neighbors detail Area (null): <table><thead><tr><th>System Id</th><th>Type</th><th>IP Address</th><th>State</th><th>Holdtime</th><th>Circuit</th><th>Interface</th></tr></thead><tbody><tr><td rowspan="2">r1</td><td>L1</td><td>1.0.0.2</td><td>Up</td><td>9</td><td>r1.01</td><td>GigabitEthernet 0/0</td></tr><tr><td>L2</td><td>1.0.0.2</td><td>Up</td><td>9</td><td>r1.01</td><td>GigabitEthernet 0/0</td></tr></tbody></table> Adjacency ID: 1 Uptime: 00:06:25 Area Address(es): 49.1111 SNPA: 00d0.f8bc.de08 IPv6 Address(es): fe80::2a9:15ff:fe36:5413							System Id	Type	IP Address	State	Holdtime	Circuit	Interface	r1	L1	1.0.0.2	Up	9	r1.01	GigabitEthernet 0/0	L2	1.0.0.2	Up	9	r1.01	GigabitEthernet 0/0
System Id	Type	IP Address	State	Holdtime	Circuit	Interface																					
r1	L1	1.0.0.2	Up	9	r1.01	GigabitEthernet 0/0																					
	L2	1.0.0.2	Up	9	r1.01	GigabitEthernet 0/0																					

	Level-1 MTID: Standard Level-2 MTID: Standard Level-1 Protocols Supported: IPv4, IPv6 Level-2 Protocols Supported: IPv4, IPv6 BFD(IPv4) session state: Up BFD(IPv6) session state: Up	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.80 show isis virtual-neighbors

	Use this command to display the virtual system neighbor information of an IS-IS system.																									
	show isis [tag] virtual-neighbors																									
Parameter Description	Parameter	Description																								
	tag	IS-IS instance.																								
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode																									
Default Level	14																									
Usage Guide	N/A																									
Configuration Examples	FS# show isis virtual-neighbors Area (null): <table><thead><tr><th>Virtual System Id</th><th>Type</th><th>State</th></tr></thead><tbody><tr><td rowspan="2">1111.1111.1111</td><td>L1</td><td>DOWN</td></tr><tr><td>L2</td><td>UP</td></tr><tr><td rowspan="2">2222.2222.2222</td><td>L1</td><td>DOWN</td></tr><tr><td>L2</td><td>UP</td></tr></tbody></table> Field description: <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Area</td><td>Instance tag</td></tr><tr><td>Virtual System Id</td><td>Virtual system ID</td></tr><tr><td>Type</td><td>Neighbor type</td></tr><tr><td>State</td><td>Neighbor status. UP indicates the level at which the</td></tr></tbody></table>			Virtual System Id	Type	State	1111.1111.1111	L1	DOWN	L2	UP	2222.2222.2222	L1	DOWN	L2	UP	Field	Description	Area	Instance tag	Virtual System Id	Virtual system ID	Type	Neighbor type	State	Neighbor status. UP indicates the level at which the
Virtual System Id	Type	State																								
1111.1111.1111	L1	DOWN																								
	L2	UP																								
2222.2222.2222	L1	DOWN																								
	L2	UP																								
Field	Description																									
Area	Instance tag																									
Virtual System Id	Virtual system ID																									
Type	Neighbor type																									
State	Neighbor status. UP indicates the level at which the																									

		extended LSP fragment is created.

4.81 show isis protocol

	Use this command to display relevant protocol information about an IS-IS system. show isis [tag] protocol	
Parameter Description	Parameter	Description
	tag	IS-IS instance.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example displays relevant protocol information about an IS-IS system. <pre> FS# show isis protocol IS-IS Router: (null) Binding VRF: vrf Mib-Binding: off System ID: 0000.0000.0036 IS-type: level-1-2 Virtual System ID: 1111.1111.1111, 2222.2222.2222 Manual area address(es): 49.0001, 49.0003 Interfaces supported by IS-IS: GigabitEthernet 0/0, GigabitEthernet 0/1 Redistributing IPv4: isis 1, isis 2 Redistributing IPv6: isis 3, isis 4 Distance: 115 Generate narrow metrics: Level-1-2 Accept narrow metrics: Level-1-2 Generate wide metrics: none Accept wide metrics: none Two-way-maintain: enable </pre> Field description:	

Field	Description
IS-IS Router	Instance tag
Binding VRF	Name of the VRF bound to the instance
Mib-Binding	Indicates whether the instance is bound with SNMP.
System ID	System ID
IS-type	Level type supported by the instance
Virtual System ID	Extended system ID
Manual area address(es)	Area ID
Interfaces supported by IS-IS	Interface associated with the instance
Redistributing IPv4	Source of redistributed IPv4 routes
Redistributing IPv6	Source of redistributed IPv6 routes
Distance	IS-IS management weight
Generate narrow metrics	Type of the generated narrow metrics
Accept narrow metrics	Type of the accepted narrow metrics
Generate wide metrics	Type of the generated wide metrics
Accept wide metrics	Type of the accepted wide metrics
Two-way-maintain	Indicates whether the two-way maintenance function enabled for the instance.

4.82 show isis topology

	Use this command to display the topology of the IS-IS router connection.	
	show isis [<i>tag</i>] topology [<i>WORD</i> all] [I1 I2 level-1 level-2]	
Parameter Description	Parameter	Description
	tag	Specifies the IS-IS instance.
	WORD	System ID or host name.
	self-originate	Displays the topology of the device.
	all	Displays the topology whose root node is the local device or the IS-IS neighbor.
	I1	Specifies the topology of Level-1.
	level-1	Specifies the topology of Level-1.
	I2	Specifies the topology of Level-2.
	level-2	Specifies the topology of Level-2.
Defaults	N/A	
Command Mode	Privileged EXEC mode/ global configuration mode/ interface configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example displays all IS-IS neighbors:	
	<pre> FS#show isis topology Area (null): IS-IS paths to level-1 routers System Id Metric Next-Hop SNPA Interface r1 10 r1 00d0.f822.33ad GigabitEthernet 0/0 FS -- IS-IS paths to level-2 routers System Id Metric Next-Hop SNPA Interface r1 10 r1 00d0.f822.33ad GigabitEthernet 0/0 FS -- </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5 BGP4 Commands

5.1 address-family ipv4

	Use this command to enter IPv4 address family configuration mode to configure BGP configuration mode. Use the no or default form of this command to exit BGP address configuration mode. address-family ipv4 [unicast multicast] no address-family ipv4 [unicast multicast] default address-family ipv4 [unicast]	
Parameter Description	Parameter	Description
	unicast	Optional, detailed IPv4 unicast address prefix
Defaults	The configuration mode is unicast address prefix by default.	
Command Mode	BGP configuration mode	
Usage Guide	In BGP address configuration mode, use the standard IPv4 address for the configuration. To return to BGP configuration mode, run the command exit-address-family.	
Configuration Examples	The following example enters the IPv4 address family configuration mode. <pre> FS(config)# router bgp 65000 </pre>	

	FS(config-router)# address-family ipv4	
Related Commands	Command	Description
	exit-address-family	Exits the mode.
Platform Description	None	

5.2 address-family ipv4 vrf

	Use this command to enter the IPv4 VRF address family configuration mode to configure BGP and enable the exchange of route information of a VRF. Use the no or default form of this command to restore the default setting. address-family ipv4 vrf vrf-name no address-family ipv4 vrf vrf-name default address-family ipv4 vrf vrf-name	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
Defaults	No vrf is defined by default.	
Command Mode	BGP configuration mode	
Usage Guide	You can execute this command to configure or exit the exchange of route information between PEs and CEs. To return to BGP configuration mode, run the exit-address-family command. If IPv4 VRF and IPv6 VRF address family modes of the same VRF are activated at the same time, and the same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both address family modes at the same time, while its address family commands will be displayed only under respective address family modes.	
Configuration Examples	The following example enters the IPv4 VRF address family configuration mode. <pre>FS(config)# router bgp 65000 FS(config-router)# address-family ipv4 vrf vpn1</pre>	
Related Commands	Command	Description
	exit-address-family	Exits the configuration mode.
Platform Description	N/A	

5.3 address-family ipv6

	Use this command to enter IPv6 address family configuration mode and enable the exchange of IPv6 route information. Use the no or default form of this command to restore the default setting. Use the exit-address-family command to exit BGP address-family configuration mode. address-family ipv6 [unicast] no address-family ipv6 [unicast] default address-family ipv6 [unicast]	
Parameter	Parameter	Description
Description	unicast	Optional, enters IPv6 unicast address-family configuration mode.
Defaults	The configuration mode is unicast address prefix by default.	
Command Mode	BGP configuration mode or BGP Scope configuration mode	
Usage Guide	You can use this command not only to enter IPv6 address-family configuration mode of the BGP to configure the IPv6 neighbors, but also activate neighbors in IPv6 address-family configuration mode after configuring IPv6 neighbors in BGP configuration mode. The exit-address-family command is used to return to BGP configuration mode.	
Configuration Examples	The following example enters the IPv6 address family configuration mode. <pre>FS(config)# router bgp 65000 FS(config-router)# address-family ipv6</pre>	
Related Commands	Command	Description
	exit-address-family	Exits the mode.
Platform Description	None	

5.4 address-family ipv6 vrf

	Use this command to enter BGP configuration mode, enable the IPv6 route information exchange function under a vrf. Use no or default form of this command to restore the default setting. Use the exit-address-family command to exit BGP address configuration mode. address-family ipv6 vrf vrf-name no address-family ipv6 vrf vrf-name default address-family ipv6 vrf vrf-name	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name

Defaults	No vrf address family is defined by default.				
Command Mode	BGP configuration mode				
Usage Guide	You can use this command to start configuring (or quit) the exchange of BGP route information between PE or MCE device and CE. You can use the <code>exit-address-family</code> command to return to BGP configuration mode.  If ipv4 vrf and ipv6 vrf address family modes of the same vrf are activated at the same time, and same neighbor is activated in two address family modes, the neighbor's global commands will be displayed in both the address family modes at the same time, while its address family commands will only be displayed under respective address family mode.				
Configuration Examples	The following example enters the IPv6 VRF address family configuration mode. <pre>FS(config)# router bgp 65000 FS(config-router)# address-family ipv6 vrf vpn1</pre>				
Configuration Examples	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>exit-address-family</td><td>Exits the mode.</td></tr> </table>	Command	Description	exit-address-family	Exits the mode.
Command	Description				
exit-address-family	Exits the mode.				
Platform Description	N/A				

5.5 address-family l2vpn

	Use this command to enter the L2VPN address family configuration mode and enable the exchange of L2VPN route information between BGP neighbors. Use the <code>no</code> or <code>default</code> form of this command to restore the default settings. address-family l2vpn {evpn} no address-family l2vpn {evpn} default address-family l2vpn {evpn}	
Parameter Description	Parameter	Description
	evpn	L2VPN EVPN address family.
Defaults	No L2VPN address family is defined by default.	
Command Mode	BGP configuration mode / BGP scope global configuration mode	

Usage Guide	Use the exit-address-family command to exit the L2VPN address family configuration mode.					
Configuration Examples	The following example enters the L2VPN VPLS address family configuration mode. FS(config)# router bgp 100 FS(config-router)# address-family l2vpn vpls					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

5.6 advertise ipv4 unicast

	Use this command to configure IPv4 VRF re-distribution. Use the no form of this command to disable the IPv4 VRF re-distribution. Use the default form of this command to restore the default settings. advertise ipv4 unicast no advertise ipv4 unicast default advertise ipv4 unicast	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The IPv4 VRF re-distribution function is disabled by default.	
Command Mode	BGP L2VPN EVPN address family mode.	
Usage Guide	Limitations on re-distribution of IPv4 unicast routes into BGP: 1. The re-distribution of IPv4 unicast routes into BGP function can only take effect in BGP L2VPN EVPN address family mode. 2. Only after the VXLAN module has advertised the L3 virtual MAC address, the IPv4 unicast routes can be re-distributed. 3. Only after the route-target import attribute of EVI instance matches the route-target attribute of VRF, the IPv4 unicast routes can be re-distributed. 4. The non-VRF IPv4 unicast routes cannot be re-distributed.	
Configuration Examples	The following example configures the re-distribution of IPv4 unicast routes into BGP. FS(config)# router bgp 65000 FS(config-router)# address-family l2vpn evpn FS(config-router-af)# advertise ipv4 unicast	
Related Commands	Command	Description
	N/A	N/A

Platform	
Description	N/A

5.7 advertise ipv6 unicast

	Use this command to configure IPv4 VRF re-distribution. Use the no form of this command to disable the IPv4 VRF re-distribution. Use the default form of this command to restore the default settings. advertise ipv6 unicast no advertise ipv6 unicast default advertise ipv6 unicast	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The IPv6 VRF re-distribution function is disabled by default.	
Command		
Mode	BGP L2VPN EVPN address family mode.	
Usage Guide	Limitations on re-distribution of IPv6 unicast routes into BGP: 1. The re-distribution of IPv6 unicast routes into BGP function can only take effect in BGP L2VPN EVPN address family mode. 2. Only after the VXLAN module has advertised the L3 virtual MAC address, the IPv6 unicast routes can be re-distributed. 3. Only after the route-target import attribute of EVI instance matches the route-target attribute of VRF, the IPv6 unicast routes can be re-distributed. 4. The non-VRF IPv6 unicast routes cannot be re-distributed.	
Configuration Examples	The following example configures the re-distribution of IPv6 unicast routes into BGP. <pre>FS(config)# router bgp 65000 FS(config-router)# address-family l2vpn evpn FS(config-router-af)# advertise ipv6 unicast</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform		
Description	N/A	

5.8 aggregate-address (IPv4)

	Use this command to set the aggregate IPv4 route. Use the no or default form of this command to restore the default setting. aggregate-address ip-address mask [as-set] [summary-only] [attribute-map map-tag] no aggregate-address ip-address mask default aggregate-address ip-address mask	
Parameter Description	Parameter	Description
	ip address	IP address of the aggregate route
	mask	Mask of the aggregate route
	as-set	Keeps the AS path information of the path in the aggregate address range.
	summary-only	Advertises only the aggregate route.
	attribute-map	Configures the routing policy to control the route attribute.
	map-tag	Route map name. Up to 32 characters is allowed.
Defaults	The address aggregation is not configured by default.	
Command Mode	BGP configuration mode, IPv4 address family configuration mode, or IPv4 VRF address family configuration mode	
Usage Guide	The BGP-enabled device will advertise all path information both before and after aggregation by default. Use the aggregate-address summary-only command to advertise the aggregate route only.	
Configuration Examples	The following example sets the aggregate IPv4 route. <pre>FS(config)# router bgp 65000 FS(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
Platform Description	None	

5.9 bgp advertise non-transitive extcommunity

	Use this command to allow carried non-transitive extcommunity when BGP is notifying EBGP neighbors of a route. Use the no or default form of this command to restore the default setting.
	bgp advertise non-transitive extcommunity
	no bgp advertise non-transitive extcommunity
	default bgp advertise non-transitive extcommunity

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Non-transitive extcommunity is removed when notifying EBGp neighbors of a route.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	By default, when notifying EBGp neighbors of a route, neighbors will not be notified of extcommunity with the "non-transitive" flag. This configuration can enable the notification of non-transitive extcommunity.  Non-transitive extcommunity will be carried when notifying alliance EBGp or IBGP neighbors of a route.	
Configuration Examples	The following example allows carried non-transitive extcommunity. <pre>FS(config)# router bgp 65000 FS(config-router)# bgp advertise non-transitive extcommunity</pre>	
Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.
Platform Description	N/A	

5.10 bgp always-compare-med

	Use this command to compare Multi Exit Discriminator (MED) all the time. Use the no or default form of this command to restore the default setting. bgp always-compare-med no bgp always-compare-med default bgp always-compare-med	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	MED of peer paths from the same AS is compared by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	The MED value is compared for paths of peers from the same AS by default. This command can be used to allow comparing MED values for paths from different ASs. If there are multiple valid paths to the same destination, the one with lower MED value has higher priority.	

	This command is not recommended unless you are sure that different ASs are using the same IGP and routing method.	
Configuration Examples	The following example compares Multi Exit Discriminator (MED) all the time.	
	<pre>FS(config)# router bgp 65000 FS(config-router)# bgp always-compare-med</pre>	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp bestpath med confed	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
	bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
	bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.
Platform Description	None	

5.11 bgp asnotation dot

	Use this command to modify the displaying mode of the 4-byte AS notation and the matching type of the regular expression as the dot mode (that is, two dotted decimal numbers). Use the no or default form of this command to restore the default setting. bgp asnotation dot no bgp asnotation dot default bgp asnotation dot	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The 4-byte AS notation is shown in decimal digit, and the regular expression also matches the 4-byte AS notation with decimal digit by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	Our devices support two modes of representing the 4-byte AS notation. One is decimal digit, and the other one is dot mode which represents the 65536 with 1.0. The decimal format is same as the default format, which represents the 4-byte AS notation with decimal digits. The dot mode displays the 4-byte AS notation in the format of ([two high bytes.] two low bytes). If the [two high bytes.] is zero, it will not be displayed. That is, the AS notation represented as 65536 in decimal is 1.0 in the dot mode. In another example, the AS notation is 65534 represented in decimal, while it is represented as 65534 in the dot mode without the zero in front. No matter which mode will be adopted to display the 4-byte AS notation, both modes can be used when	

	entering the configuration commands. But the representation and displaying mode of the 4-byte AS notation in the regular expression must be the same. Otherwise, the matching will fail. After executing the bgp asnotation command, you must use the clear ip bgp * to perform the resetting, so as to re-match the filtering condition of the regular expression.  The AS notation is represented as 1 to 65535 no matter using decimal or dot mode.					
Configuration Examples	The following example modifies the showing mode of the 4-byte AS notation. <pre>FS(config)# router bgp 1.0 FS(config-router)# bgp asnotation dot</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip bgp summary</td><td>Displays the related information of BGP neighbor.</td></tr></table>	Command	Description	show ip bgp summary	Displays the related information of BGP neighbor.	
Command	Description					
show ip bgp summary	Displays the related information of BGP neighbor.					
Platform Description	None					

5.12 bgp bestpath as-path ignore

	Use this command to disregard the length of the AS path. Use the no or default form of this command to restore the default setting. bgp bestpath as-path ignore no bgp bestpath as-path ignore default bgp bestpath as-path ignore	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The AS path length is considered in choosing the optimal path by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	BGP will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path into account when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.	
Configuration Examples	The following example disregard the length of the AS path. FS(config)# router bgp 65000 FS(config-router)# bgp bestpath as-path ignore	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.13 bgp bestpath as-path multipath-relax

	Use this command to enable AS path multipath-relax (only comparing the AS path length) for BGP multipathing load. Use the no or default form of this command to restore the default setting.	
	bgp bestpath as-path multipath-relax	
	no bgp bestpath as-path multipath-relax default bgp bestpath as-path multipath-relax	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	BGP requires that AS path attributes must be the same when calculating equal-cost multipath (ECMP) by default.	
Defaults	BGP configuration mode / Scope global configuration mode	
Usage Guide	BGP compares AS path attributes in a precise way when selecting the optimal path as ECMP by default. Only paths with same AS path attributes can constitute equal-cost paths. As a result, BGP multipathing load balancing cannot be implemented in an application scenario. After AS path multipath-relax is enabled, only the AS path length is compared, allowing the implementation of BGP multipathing load balancing.	
Configuration Examples	The following example enables AS path multipath-relax for BGP multipathing load. <pre>FS(config)# router bgp 65530 FS(config-router)# bgp bestpath as-path multipath-relax</pre>	
Related Commands	Command	Description
	router bgp	Enables BGP.
	show ip bgp	Displays BGP routing entries.
Platform Description	None	

5.14 bgp bestpath compare-confed-aspeth

	Use this command to compare the AS path length of the confederation from the same external routes when selecting the optimal path, with smaller AS path in the confederation for higher path priority. Use the no or default form of this command to restore the default setting.	
	bgp bestpath compare-confed-aspeth no bgp bestpath compare-confed-aspeth default bgp bestpath compare-confed-aspeth	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	The AS path of the EBGP peer routes inside the same confederation is not compared by default when selecting the optimal path. Instead, the routing method is implemented.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	During the selection of the same routing information from the peer of the internal EBGP By default, the AS path of the confederation is not compared. This command is used to compare the AS path of the confederation. Note that if a route contain no AS path of the confederation, it is impossible to implement the AS path comparison for that route.	
Configuration Examples	The following example compares the AS path length of the confederation. FS(config)# router bgp 65000 FS(config-router)# bgp bestpath compare-confed-asp	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp router-id	Sets the BGP Device ID.
Platform Description	None	

5.15 bgp bestpath compare-routerid

	Use this command to compare the router ID of the same external routes when selecting the optimal path, with smaller router ID for higher path priority. Use the no or default form of this command to restore the default setting. bgp bestpath compare-routerid no bgp bestpath compare-routerid default bgp bestpath compare-routerid	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	If two paths received from different EBGP peers have the same path, the first one is considered with higher priority by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	If two paths with identical path attributes are received from different EBGP peers during the selection of the optimal path, we will select the optimal path according to the sequence of receiving the paths by default. You can select the path with smaller Device ID as the optimal path by configuring the following commands.	

Configuration Examples	The following example compares the router ID of the same external routes.	
	<pre>FS(config)# router bgp 65000 FS(config-router)# bgp bestpath compare-routerid</pre>	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp router-id	Sets the BGP Device ID.
Platform Description	None	

5.16 bgp bestpath med confed

	Use this command to compare the MED value of the path of the internal peer from AS confederation during selecting the optimal path. Use the no or default form of this command to restore the default setting. bgp bestpath med confed [missing-as-worst] no bgp bestpath med confed [missing-as-worst] default bgp bestpath med confed [missing-as-worst]	
Parameter Description	Parameter	Description
	missing-as-worst	Sets the priority of the path without MED attribute as the lowest.
Defaults	The MED value of the path of the peer inside the AS confederation is not compared by default when selecting the optimal path.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	The MED attribute of the path is transferred between the ASs inside the confederation. You may set always comparing this value.	
Configuration Examples	The following example compares the MED value of the path of the internal peer.	
	<pre>FS(config)# router bgp 65000 FS(config-router)# bgp bestpath med confed</pre>	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
	bgp bestpath med missing-as-worst	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
	bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.

Platform	
Description	None

5.17 bgp bestpath med missing-as-worst

	Use this command to set the priority of the path without MED attribute as the lowest when selecting the optimal path. Use the no or default form of this command to restore the default setting. bgp bestpath med missing-as-worst no bgp bestpath med missing-as-worst default bgp bestpath med missing-as-worst	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	If a path without MED attribute is received, the MED value of the path is 0 by default. Such route has the highest priority according to the above-mentioned rule.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	The MED value of a path without MED attribute will be 0 by default. For the smaller the MED value, the higher the priority of the path is, the MED value of this path has the highest priority. This command can be used to figure the path without MED attribute has the lowest priority.	
Configuration Examples	The following example sets the priority of the path without MED attribute as the lowest. <pre>FS(config)# router bgp 65000 FS(config-router)# bgp bestpath medmissing-as-worst</pre>	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
	bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.
	bgp deterministic-med	Compares paths of peers from the same AS when selecting the optimal path.
Platform		
Description	None	

5.18 bgp bestpath multipath-compare-routerid

	Use this command to enable the router ID comparison among multiple BGP paths. Load balancing can be implemented only when multiple paths (same router ID) are from the same device. Use the no form of this command to disable the router ID comparison among multiple BGP paths. Use the default form of this

	command to restore the default settings. bgp bestpath multipath-compare-routerid no bgp bestpath multipath-compare-routerid default bgp bestpath multipath-compare-routerid	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The router ID comparison among multiple BGP paths is disabled by default.	
Command Mode	BGP configuration mode, BGP Scope Global Configuration Mode	
Default Level	14	
Usage Guide	N/A	
Configuration Example	The following example enables the router ID comparison among multiple BGP paths. <pre>FS(config)# router bgp 65000 FS(config-router)# bgp bestpath multipath-compare-routerid</pre>	
Verification	Run the show running-config command to display the BGP configuration.	

5.19 bgp client-to-client reflection

	Use this command to enable the route reflection function between clients on the device. Use the no or default form of this command disables the route reflection function between clients. bgp client-to-client reflection no bgp client-to-client reflection default bgp client-to-client reflection	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled without the client for route reflection by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	In general, it is unnecessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the route among clients. However, if the full connection relationship is established for all clients, the function for the route reflector to reflect the client route can be	

	disabled. To disable the route reflection function, use the command no bgp client-to-client reflection .	
Configuration Examples	The following example shows how to enable the route reflection function between clients on the device. <pre>FS(config)# router bgp 65000 FS(config-router)# no bgp client-to-client reflection</pre>	
Related Commands	Command	Description
	bgp cluster-id	Configures the cluster ID of the route reflector.
	neighbor route-reflector-client	Configures the client of the route reflector and configure itself as the route reflector.
Platform Description	None	

5.20 bgp cluster-id

	Use this command to configure the cluster ID of the route reflector. Use the no or default form of this command to restore it to the default setting. bgp cluster-id cluster-id no bgp cluster-id default bgp cluster-id	
Parameter Description	Parameter	Description
	<i>cluster-id</i>	Cluster ID of the route reflector, an IP address of up to four bytes or an integer (must be entered in form of IP address)
Defaults	The cluster id is the router-id of the route reflector by default.	
Command Mode	BGP configuration mode / Scope global configuration mode	
Usage Guide	In general, one group is only configured with one route reflector. In this case, the Device ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.	
Configuration Examples	The following example configures the cluster ID of the route reflector. <pre>FS(config)# router bgp 65000 FS(config-router)# bgp cluster-id 10.0.0.1</pre>	
Related Commands	Command	Description
	bgp client-to-client	Configures the route reflection between clients.

	reflection	
	neighbor route-reflector-client	Configures the client of the route reflector and configures itself as the route reflector.
Platform		
Description	None	

5.21 bgp confederation identifier

	Use this command to configure the AS confederation identifier. Use the no or default form of this command to restore the default setting. bgp confederation identifier as-number no bgp confederation identifier default bgp confederation identifier	
Parameter Description	Parameter	Description
	<i>as-number</i>	AS confederation identifier in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, which is represented as 1 to 65535.65535 in dot mode.
Defaults	There is no confederation identifier by default	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	The confederation is a measure to reduce the connections of IBGP peers within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. For the external confederation, the whole confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information.	
Configuration Examples	The following example configures the AS confederation identifier. <pre>FS(config-router)# bgp confederation identifier 65000</pre>	
Related Commands	Command	Description
	bgp confederation peers	Adds member AS of the AS confederation.
Platform Description	None	

5.22 bgp confederation peers

	Use this command to configure member ASs of the AS confederation. Use the no or default form of this command to restore the default setting. bgp confederation peers as-number [...as-number] no bgp confederation peers as-number [...as-number] default bgp confederation peers [as-number [...as-number]]	
Parameter Description	Parameter	Description
	<i>as-number</i>	Member ASs in the confederation range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
Defaults	There is no confederation member by default.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	The confederation is a measure to reduce the connections of BGP peers within the AS. One AS is divided into several sub ASs and one unified confederation ID (namely, confederation AS number) is set to constitute these sub ASs into a confederation. The whole external confederation is still considered as one AS, and only the confederation AS number is visible for the external network. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers within the sub AS, and the EBGP connection is established among the BGP Speakers within the sub AS. Despite of the EBGP connections established between the BGP speakers in an AS, the next-hop, MED and local priority information remains unchanged in exchanging the information. This command is used to specify the member AS of a confederation.  This command can configure up to 25 members of a confederation at one time. For more members, enter them for several times.	
Configuration Examples	The following example configures member ASs of the AS confederation. <pre>FS(config-router)# bgp confederation peers 65000 65100</pre>	
Related Commands	Command	Description
	bgp confederation identifier	Configures the confederation identifier.
Platform Description	None	

5.23 bgp dampening

	Use this command to enable the routing attenuation and set the attenuation parameters in the address-family or routing configuration mode. Use the no or default form of this command to restore the default setting.

	bgp dampening [half-life [reusing suppressing duration] route-map name] no bgp dampening default bgp dampening	
Parameter Description	Parameter	Description
	<i>half-life</i>	Half-life period, ranging from 1 to 45 minutes
	<i>reusing</i>	When the penalty value reaches this value, the routing suppression is cancelled. The value ranges from 1 to 10000.
	<i>suppressing</i>	When the penalty value reaches this value, routing is suspended. The value ranges from 1 to 20000.
	<i>duration</i>	Maximum time for routing suppression, ranging from 1 to 255 minutes
	<i>name</i>	Route-map name, apply the routing attenuation to the specified route through the route-map.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4 unicast address-family configuration mode, BGP IPv4 VRF address-family configuration mode, BGP IPv6 unicast address-family configuration mode, BGP IPv6 VRF address-family configuration mode, BGP L2VPN EVPN address-family configuration mode and BGP Scope configuration mode	
Usage Guide	The bgp dampening command is used to suppress unstable EBGp routes and does not take effect to IBGP routes. The BGP uses the penalty value to describe the route stability. A larger penalty value indicates a more unstable route. The penalty value increases by 1000 when route oscillation occurs (upon receiving withdraw packets). The penalty value does not increase when the upper limit is reached. The upper limit is determined based on the configured duration value and calculated using the following formula: Penalty upper limit = $2^{\wedge}(\text{Duration}/\text{Half-life}) \times \text{Reusing}$. In addition, the penalty upper limit cannot be greater than 20000. Therefore, the duration, half-life, and reusing values need to be adjusted based on the network conditions. The relationship among these parameters are as follows: Half-life $\leq$ Duration Reusing $\leq$ Suppressing $\leq$ Penalty upper limit You can also specify only the half-life value. In this case, the duration value is (half-life x 4), the reusing value is 750, and the suppressing value is 2000. EBGP routes whose penalty value exceeds the suppressing value will be suppressed. Suppressed routes will not be used during BGP route election and will not be advertised to other BGP peers. If route oscillation occurs in suppressed routes, the penalty value will continue to increase until the penalty upper limit is reached. The penalty value of suppressed routes will decrease by a half each time the half-life time passes. When the penalty value decreases to the reusing value, routes whose attribute is update in the last update will participate in BGP route election again. When the penalty value decreases to 0, routes whose attribute is withdraw in the last update will be deleted from the BGP route table.	
Configuration Examples	The following example enables the routing attenuation and set the attenuation parameters. <pre>FS(config-router)# bgp dampening 30 1500 10000 120</pre>	

Related Commands	Command	Description
	clear ip bgp dampening	Clears the BGP suppression and cancels the suppression for the routes.
	show ip bgp dampening dampened-paths	Displays the suppressed route information.
Platform Description	None	

5.24 bgp default ipv4-unicast

	Use this command to set the IPv4 unicast address as the default address family. Use the no or default form of this command to restore the default setting. bgp default ipv4-unicast no bgp default ipv4-unicast default bgp default ipv4-unicast	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	The IPv4 unicast address is the default address family.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	This command is used to set the default address family of BGP as the IPv4 unicast address.	
Configuration Examples	The following example sets the IPv4 unicast address as the default address family. <pre>FS(config-router)#bgp default ipv4-unicast</pre>	
Related Commands	Command	Description
	address-family ipv4	Enters the IPv4 address mode.
Platform Description	None	

5.25 bgp default local-preference

	Use this command to set the default local-preference attribute value. Use the no or default form of this command to restore the default setting. bgp default local-preference value no bgp default local-preference default bgp default local-preference	
Parameter	Parameter	Description
Description	<i>value</i>	Local priority attribute, in the range from 0 to 4294967295

Defaults	The local preference value is 100 by default.	
Command Mode	BGP configuration mode or BGP Scope configuration mode.	
Usage Guide	The BGP takes the local preference as the foundation to compare with the priority of the path learned from IBGP peers. The larger the local preference value, the higher the priority of the path is. The BGP speaker sends the external route received to the IBGP peers to add the local priority value.	
Configuration Examples	The following example sets the default local-preference attribute value.	
	FS(config-router)# bgp default local-preference 200	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp always-compare-med	Allows comparing the MED value of the path of the peer from different ASs when electing the optimal path.
	bgp bestpath med confed	Allows comparing the MED value of paths of internal peers from AS community when electing the optimal path.
	bgp bestpath med missing-as-worst	Allows setting the priority of the path without MED attribute as the lowest when electing the optimal path.
Platform Description	None	

5.26 bgp default route-target filter

	Use this command to enable the route-target filtering. For the VPNV4 routes, filter the community attributes of the route-target by default. Use the no or default form of this command to disable this function. bgp default route-target filter no bgp default route-target filter default bgp default route-target filter	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	BGP configuration mode, VPNv4/VPNv6 address-family configuration mode, BGP L2VPN EVPN address-family configuration mode or BGP Scope Global configuration mode.	
Usage Guide	After receiving the VPNV4 route, use the community attributes list of the route-target to filter and distribute different VRFs. With the no form of this command used, the BGP will receive all VPNV4 routes no matter whether these filtered VPNV4 routes will be received by route-target of local VRF.	

	With the PE route-reflector-client configured for the BGP, the VPNV4 route will not be processed through the route-target filtering. In this case, whether the BGP is enabled, the actions are the same without the route-target filtering.	
Configuration Examples	The following example enables the route-target filtering. <pre>FS(config)# router bgp 65000 FS(config-router)# no bgp default route-target filter</pre>	
Related Commands	Command	Description
	neighbor route-reflector-client	Configures the route-reflector-client, and sets itself as the route reflector.
Platform Description	N/A	

5.27 bgp deterministic-med

	Use this command to set comparing preferentially the MED values of peer paths from the same AS. By default, the comparison is based on the received order, and the one received the last is compared first. Use the no or default form of this command to restore the default setting. bgp deterministic med no bgp deterministic med default bgp deterministic-med	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	They will be compared with each other according to the sequence the paths are received when the optimal path is selected by default. Execute the following operations in the BGP configuration mode to compare paths of peers from the same AS firstly:	
Configuration Examples	The following example sets the comparing preferentially MED values. <pre>FS(config-router)# bgp deterministic med</pre>	
Related Commands	Command	Description
	show ip bgp	Displays the BGP route entry.
	bgp always-compare-med	Compares the MED value of paths of peers from different ASs when selecting the optimal path.
	bgp bestpath med confed	Sets the priority of the path without MED attribute as the lowest when selecting the optimal path.

	bgp bestpath med missing-as-worst	Compares paths of peers from the same AS when selecting the optimal path.
Platform Description	None	

5.28 bgp enforce-first-as

	Use this command to reject the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. Use the no or default form of this command to disable this function. bgp enforce-first-as no bgp enforce-first-as default bgp enforce-first-as	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command		
Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	The AS number of the device is put into the path section by default to update the update message.	
Configuration Examples	The following example rejects the UPDATE messages whose first AS_PATH path section is not the neighbor-configured AS number. FS(config-router)# bgp enforce-first-as	
Related	Command	Description
Commands	show ip bgp	Displays the BGP route entry.
Platform		
Description	None	

5.29 bgp fast-external-fallover

	When the network interface used in establishing the connection of the directly-connected EBGP peer fails, use this command to establish the BGP session connection quickly. Use the no or default form of this command to disable this function. bgp fast-external-fallover no bgp fast-external-fallover default bgp fast-external-fallover	
Parameter	Parameter	Description
Description	N/A	N/A

Defaults	This function is enabled by default.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	This command takes effect only for the directly-connected EBGP neighbor.	
Configuration Examples	The following example creates the fast BGP session. FS(config-router)# bgp faster-external-falover	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
Platform Description	None	

5.30 bgp fast-reroute

	Use this command to enable BGP Fast Reroute. Use the no or default form of this command to restore the default setting. bgp fast-reroute no bgp fast-reroute default bgp fast-reroute	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode/ BGP IPv4 unicast address family configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP scope global configuration mode.	
Usage Guide	 The BGP Fast Reroute function is supported in the BGP IPv4 unicast address family configuration mode and the BGP IPv4 VRF address family configuration mode.  Only one backup route will be generated and the next-hop of this backup route cannot be the same as that of the preferred route.  When ECMP is enabled, the FRR cannot generate backup route.  When this function is enabled in the BGP IPv4 VRF address family configuration mode, the priority of BGP FRR is lower than that of VPN FRR. So when the VPN FRR is enabled in IPv4 VRF configuration mode, BGP FRR does not take effect unless VPN FRR is unable to calculate the backup route.	
Configuration	The following example enables BGP Fast Reroute.	

Examples	FS(config)# router bgp 65530 FS(config-router)# bgp faster-reroute	
Related	Command	Description
Commands	N/A	N/A
Platform		
Description	N/A	

5.31 bgp graceful-restart

	Use this command to enable the global BGP graceful restart function. Use the no or default form of this command to disable BGP graceful restart. bgp graceful-restart no bgp graceful-restart default bgp graceful-restart	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	By default, BGP graceful restart is enabled so as to help neighbors to perform graceful restart.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	The ability of the BGP is advertised and negotiated through the ability field of the Open message. The ability is negotiated during initially setting up the connection. So both sides must reach the consistency of the ability. If it is not supported by any side, this router device will perform the GR incorrectly. With the GR function enabled, the connected Open message will carry the GR ability field to perform the negotiation of the GR ability. To implement the GR correctly, the GR function must be enabled on both sides of the neighbors.  This command does not take effect immediately on all BGP connections that are set up successfully. To negotiate the GR ability immediately, you need to restart the BGP connection to make the local device negotiate the GR ability with the Peer again by using the clear ip bgp command. The BGP graceful-restart is used to forward data continuously of the whole network, it requires the device to keep the BGP routing entry valid and forward data continuously when restarting the BGP protocol. Supporting the continuous forwarding during the restarting is related to the hardware ability.	
Configuration Examples	The following example enables the graceful restart function of the global BGP. <pre>FS(config)# router bgp 500 FS(config-router)# bgp graceful-restart</pre>	

Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	bgp graceful-restart restart-time	Configures the restart time of the BGP graceful-restart.
Platform		
Description	N/A	

5.32 bgp graceful-restart disable

	Use this command to disable GR capability of a BGP address family. Use the no or default form of this command to restore the default setting.	
	bgp graceful-restart disable	
	no bgp graceful-restart disable default bgp graceful-restart disable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The function is enabled by default.	
Command Mode	BGP configuration mode, IPv4 unicast address family mode, VPNv4 address family mode, VPNv4 address family mode, BGP L2VPN EVPN address-family configuration mode or BGP Scope configuration mode	
Usage Guide	When BGP GR function is enabled, the GR capability for all address families is enabled by default, except for address families that do not support GR capability. After GR capability is enabled, you can use this command in the address family mode to disable the address family's GR capability. The Configuration of this command in BGP mode is effective on IPv4 Unicast address family. When BGP GP function is disabled, GR capability is disabled for all address families.	
Configuration Examples	The following example disables the graceful restart function of the BGP IPv4 address family. <pre>FS(config)# router bgp 65000 FS(config-router)# bgp graceful-restart FS(config-router)# address-family ipv4 FS(config-router-af)# bgp graceful-restart disable</pre>	
Configuration Examples	Command	Description
	bgp graceful-restart	Enables BGP's GR capability.
	address-family ipv4	Enters BGP IPv4 address family mode.
Platform		
Description	N/A	

5.33 bgp graceful-restart restart-time

	Use this command to configure the restart time of the BGP graceful-restart. Use the no or default form of this command to restore the default setting. bgp graceful-restart restart-time restart-time no bgp graceful-restart restart-time default bgp graceful-restart restart-time	
Parameter Description	Parameter	Description
	<i>restart-time</i>	GR Restarter-hoped longest waiting time before re-establishing the connection between the GR Helper and the GR Restarter, in the range from 1 to 3600 in the unit of seconds.
Defaults	The default is 120.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode.	
Usage Guide	The restart time is advertised by GR Restarter to GR Helper, it is GR Restarter-hoped longest waiting time before re-establishing the connection between GR Helper and GR Restarter. After this time, if the BGP connection with GR Restarter is not in Established status, GR Helper will consider this BGP session failed and will restore the normal BGP. All the routing of the neighbor will be deleted during this period, affecting the data redistribution. The restart time is advertised in the GR ability field of the BGP Open message. The GR restart time of the two ends of the session is not required to be the same, but it is recommended.  This command does not take effect immediately on all BGP connections that are set up successfully. To advertise the newly set restart time to the GR helper, you need to restart the BGP connection to negotiate the GR ability again and advertise the restart time by using the clear ip bgp command. The configured restart time should not be greater than the Hold Time of the BGP peer, if so, the Hold time will be the restart time when the GR ability is advertised to the BGP peer.	
Configuration Examples	The following example configures the restart time of the BGP graceful-restart. <pre>FS(config)# router bgp 500 FS(config-router)# bgp graceful-restart FS(config-router)# bgp graceful-restart restart-time 150 FS(config-router)# no bgp graceful-restart restart-time</pre>	
Related Commands	Command	Description
	bgp graceful-restart	Enables the BGP graceful-restart.
Platform Description	N/A	

5.34 bgp graceful-restart stalepath-time

	Use this command to configure the time to help the device keep the route valid when executing the BGP graceful-restart. Use the no or default form of this command to restore the default setting. bgp graceful-restart stalepath-time stalepath-time time no bgp graceful-restart stalepath-time default bgp graceful-restart stalepath-time	
Parameter Description	Parameter	Description
	<i>time</i>	Longest time used to keep the stale route valid after restoring the connection with the neighbors, in the range from 1 to 3600 in the unit of seconds
Defaults	The default is 360.	
Command Mode	BGP configuration mode	
Usage Guide	This command is configured for the parameters of the GR Helper. The stalepath-time is the longest time of the GR Helper waiting to receive the EOR mark of the Restarter after restoring the connection with the GR Restarter. When the GR Helper detects that the connection with the GR Restarter fails, the original route of the Restarter is marked as the "Stale". However these routes are still used for the routing calculation and forwarding. The GR Helper updates the routes and cancels the "Stale" mark according to route updating information received from the GR Restarter. If routes marked as "Stale" are not updated in the stalepath-time period, they will be deleted. This mechanism is used to avoid failure in convergence of routes when the GR Helper fails to receive the EOR mark of the GR Restarter for a long time.	
Configuration Examples	The following example configures the restart time of the BGP graceful-restart. <pre>FS(config)# router bgp 500 FS(config-router)# bgp graceful-restart FS(config-router)# bgp graceful-restart stalepath-time 240</pre>	
Related Commands	Command	Description
	bgp graceful-restart	Enables the BGP graceful-restart.
Platform Description	N/A	

5.35 bgp initial-advertise-delay

	Use this command to configure the delay period before a BGP device sends its initial updates to peers. Use the no form or default form of this command to restore the default setting. bgp initial-advertise-delay delay-time [startup-time] no bgp initial-advertise-delay default bgp initial-advertise-delay

	Use this command to enable the BGP delayed advertisement upon system restart. Thus, the route will be immediately sent after the prefix-list policy is matched. Use the no form or default form of this command to restore the default setting. bgp initial-advertise-delay prefix-list prefix-list-name no bgp initial-advertise-delay prefix-list default bgp initial-advertise-delay prefix-list	
Parameter Description	Parameter	Description
	<i>delay-time</i>	The delay period, in seconds, before a BGP device sends its updates. The range is from 1 to 600. The default value is 1 second.
	<i>startup-time</i>	The time for the BGP device restart. In the period, the neighbor does not send its updates to peers. The range is from 5 to 584,000. The unit is second and the default value is 600 seconds.
	<i>prefix-list-name</i>	Name of the prefix-list. It cannot exceed 32 characters.
Defaults	The initial advertisement delay is disabled by default.	
Command Mode	BGP configuration mode	
Usage Guide	This command is used to configure parameters for delayed neighbor route advertisement during device restart. delay-time indicates the longest time for sending a route to a neighbor after the BGP neighbor relationship is established. In normal cases, after the neighbor relationship is established, the first route is advertised immediately and subsequent routes are advertised based on the default time. For details, see the neighbor advertisement-interval command. startup-time indicates the configurable startup time and starts to count when the configuration command takes effect. Within the time specified by startup-time, routes to BGP neighbors are advertised periodically based on delay-time. This command can be used to change the route advertisement behavior from the BGP peer to neighbors after device restart. The prefix-list policy is configured to ensure that partial routes can be normally delivered. The prefix-list policy applies to distributed routes. Matched routes will be normally delivered without being affected by delayed advertisement. For details about the address family scope to which the prefix-list policy applies, see the neighbor prefix-list command. This command is used by the administrator to adjust the BGP route advertisement behavior during device restart based on the hardware conditions, number of neighbors, number of routes, and actual deployment requirements.	
Configuration Examples	The following example configures initial delay to 60 seconds within 500 seconds after BGP restart. <pre>FS(config)# router bgp 500 FS(config-router)# bgp initial-advertise-delay 60 500</pre>	
Related Commands	Command	Description
	bgp graceful-restart	Enables the BGP graceful-restart.
Platform Description	N/A	

5.36 bgp log-neighbor-changes

	Use this command to log the BGP status changes without turning on debug. Use the no or default form of this command to disable this function. bgp log-neighbor-changes no bgp log-neighbor-changes default bgp log-neighbor-changes	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command		
Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	The debug command can also be used to log BGP status changes. But this command may consume many resources.	
Configuration	The following example logs the BGP status changes without turning on debug.	
Examples	FS(config-router)# bgp log-neighbor-changes	
Related	Command	Description
Commands	router bgp	Enables the BGP protocol.
Platform		
Description	None	

5.37 bgp maxas-limit

	Use this command to set the maximum number of ASs in the BGP AS-PATH attribute. Use the no or default form of the command to restore the default configuration. bgp maxas-limit number no bgp maxas-limit default bgp maxas-limit	
Parameter	Parameter	Description
Description	<i>number</i>	The maximum number of ASs in the BGP AS-PATH attribute. The range is from 1 to 512.
Defaults	No maximum number of ASs is set by default.	
Command		
Mode	BGP configuration mode/ BGP scope global configuration mode.	

Usage Guide	The routes exceeding the AS number limit are discarded directly, After changing the configuration, use the clear command to reset the neighbor and make the configuration take effect.				
Configuration	The following example sets the maximum number of ASs in the BGP AS-PATH attribute to 100.				
Examples	FS(config-router)# bgp maxas-limit 100				
Related					
Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform					
Description	N/A				

5.38 bgp maximum-prefix

	Use this command to restrict the maximum number of routes in the BGP global or specified VRF. Use the no or default form of the command to restore the default configuration. bgp maximum-prefix <i>numbers</i> [vrf <i>vrf-name</i>] no bgp maximum-prefix [vrf <i>vrf-name</i>] default bgp maximum-prefix [vrf <i>vrf-name</i>]						
Parameter	<table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td><i>vrf-name</i></td><td>Indicates name of a specific VRF.</td></tr> <tr> <td><i>numbers</i></td><td>Indicates number of routes. Range: 1 to 4,294,967,295.</td></tr> </table>	Parameter	Description	<i>vrf-name</i>	Indicates name of a specific VRF.	<i>numbers</i>	Indicates number of routes. Range: 1 to 4,294,967,295.
Parameter	Description						
<i>vrf-name</i>	Indicates name of a specific VRF.						
<i>numbers</i>	Indicates number of routes. Range: 1 to 4,294,967,295.						
Defaults	The function is disabled by default.						
Command							
Mode	BGP configuration mode/ BGP scope global configuration mode.						
Usage Guide	When a route advertisement in an address family causes the current number of BGP routes to exceed the maximum number, a prompt indicating route overflow in the global or specified VRF is displayed, and the BGP global or specified VRF is set to the overflow state. The BGP routing information prefix may be introduced by redistribute, from a neighbor or from another VRF. In either case, once the BGP routing information prefix of an address family is introduced, the number of BGP global or specified VRF routes reaches the upper limit, the prefix will not increase and a prompt indicating route overflow in the global or specified VRF is displayed, and the BGP global or specified VRF is set to the overflow state. Run the show bgp { addressfamily all } summary command to check routing information base status. If the address family enters the overflow state because the BGP routing information prefix reaches the upper limit, it can be adjusted by maximum-prefix. For IPv4 unicast routes, the routing information prefix may still be received if it is in the overflow state in the following cases: 1) The routing information of the same routing prefix already exists in the routing information base; 2) A route that covers the prefix (except the default route) already exists in the routing information base, and the next hop of the route is different from the next hop of the newly received route prefix.						
Configuration	The following example sets the maximum number of routes to 100.						

Examples	FS(config)#router bgp 100	
	FS(config-router)#bgp maximum-prefix 100	
Related Commands	Command	Description
	N/A	N/A
Platform		
Description	N/A	

5.39 bgp mp-error-handle session-retain

	Use this command to retain BGP sessions when BGP protocol detects errors in multi-protocol route attributes. Use the no or default form of this command to restore the default setting.	
	bgp mp-error-handle session-retain [refresh-timer time]	
	no bgp mp-error-handle session-retain	
	default bgp mp-error-handle session-retain	
Parameter Description	Parameter	Description
	refresh-timer time	Configures the waiting time for auto route recovery. The parameter ranges from 10 to 4294967296 in the unit of seconds. The default is 120.
Defaults	By default, BGP sessions will be interrupted when multi-protocol attribute errors are detected.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	By default, when UPDATA packets are received from a neighbor, BGP sessions will be interrupted if multi-protocol attribute errors are detected, which will cause oscillation of routes of all the address families of the neighbor. An address family's route error will affect the stability of routes of other address families. After this command is configured, when an error of the route attribute of an address family occurs, all the route information of the address family and neighbor will be deleted, thus preventing impact on the BGP session and other protocol address families, improving BGP protocol's stability. The option recovery-time is used to configure the waiting time for auto route recovery. To use the option, the neighbor must support the route refreshing capability. After recovery-time expires, BGP will send a route-refresh message to the neighbor's address family and re-notify the neighbor of the address family's all route information.	
Configuration Examples	The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes. <pre>FS(config-router)# bgp mp-error-handle session-retain</pre>	
Configuration Examples	Command	Description
	N/A	N/A

Platform	N/A
Description	

5.40 bgp nexthop trigger delay

	Use this command to configure the delay time for updating the routing table when the nexthop of the BGP route changes. Use the no or default form of this command to restore the default setting. bgp nexthop trigger delay delay-time no bgp nexthop trigger delay default bgp nexthop trigger delay	
Parameter Description	Parameter	Description
	<i>delay-time</i>	Delay time for updating the routing table when the nexthop changes, in the range from 0 to 100 in the unit of seconds
Defaults	The default is 5.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to configure the delay time for updating the routing table when the nexthop changes, it takes effect when the bgp nexthop trigger enable switch is opened.	
Configuration Examples	The following example retains BGP sessions when BGP protocol detects errors in multi-protocol route attributes. <pre>FS(config-router)# bgp nexthop trigger delay 30</pre>	
Related Commands	Command	Description
	bgp nexthop trigger enable	Enables the nexthop trigger.
Platform Description	None	

5.41 bgp nexthop trigger enable

	Use this command to enable the nexthop trigger update function. Use the no or default form of this command to disable this function. bgp nexthop trigger enable no bgp nexthop trigger enable default bgp nexthop trigger enable	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is enabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address-family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP VPNv4/VPNv6 address-family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to enable the nexthop trigger update function.	
Configuration Examples	The following example enables the nexthop trigger update function. FS(config-router)# bgp nexthop trigger enable	
Related Commands	Command	Description
	Bgp nexthop trigger delay	Sets the delay time for updating the routing table when the nexthop changes.
Platform Description	None	

5.42 bgp notify unsupported-capability

	Use this command to enable the neighbor address family capability detection function. Use the no or default form of this command to restore the default setting.	
	bgp notify unsupported-capability	
	no bgp notify unsupported-capability default bgp notify unsupported-capability	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	When BGP neighbor address family capability negotiation is not fully consistent, neighbors can still be connected. After this command is configured, when an address family capability supported by the local device is not supported by the neighbor device, Notification packet that carries the address family that does not support the capability will be send.	
Configuration Examples	The following example enables the neighbor address family capability detection function. FS(config)# router bgp 65000 FS(config-router)# bgp notify unsupported-capability	
Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.
Platform	N/A	

Description	

5.43 bgp redistribute-internal

	Use this command to control BGP whether to allow redistributing routes learned from IBGP, such as RIP, OSPF and ISIS, to the IGP protocol. Use the no or default form of this command to disable this function. bgp redistribute-internal no bgp redistribute-internal default bgp redistribute-internal	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	IBGP routes are allowed by default to be redistributed to the IGP protocol.	
Command Mode	BGP configuration mode, IPv4/IPv6 Unicast address family configuration mode, IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to control whether IBGP routes are allowed to be redistributed to the IGP protocol.	
Configuration Examples	The following example enables the BGP to learn the redistributing routes from IBGP. <pre>FS(config-router)# bgp redistribute-internal</pre>	
Related Commands	Command	Description
	redistribute	Redistributes routes learned from other protocols.
Platform Description	None	

5.44 bgp router-id

	Use this command to configure the ID-IP address of the device. Use the no or default form of this command to restore the default setting. bgp router-id ip-address no bgp router-id default bgp router-id	
Parameter	Parameter	Description
Description	<i>ip address</i>	IP address
Defaults	The loop-back interface of the device is selected preferentially by default. If it does not exist, the device route-id of the device is used.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope Global configuration mode.	
Usage Guide	This command is used to configure IP address, the ID of the device when running the BGP protocol.	

Configuration	The following example configures the ID-IP address of the device.	
Examples	FS(config-router)# bgp router-id 10.0.0.1	
Related Commands	Command	Description
	show ip bgp dampening dampened-paths	Displays the suppressed routing information.
	bgp dampening	Enables the route dampening function and sets dampening parameters.
Platform Description	None	

5.45 bgp scan-rib disable

	Use this command to update the routing table by event triggering. Use the no or default form of this command to restore the default setting. bgp scan-rib disable no bgp scan-rib disable default bgp scan-rib disable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	Timely scan and update is enabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address-family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP L2VPN EVPN address family configuration mode and BGP Scope configuration mode.	
Usage Guide	BGP provides two route update mechanisms: regular-scanning update and event-triggering update. Regular-scanning update indicates that BGP uses an internal timer to start scanning regularly and update the routing table. Event-triggering update indicates that BGP starts scanning and updates the routing table when the BGP configuration commands are changed due to user configuration or the next hop of a BGP route changes.	
Configuration	The following example configures the timely scan for the BGP protocol.	
Examples	FS(config-router)# bgp scan-rib disable	
Related Commands	Command	Description
	bgp scan-time	Configures the interval for the BGP timely scan.
Platform Description	None	

5.46 bgp scan-time

	Use this command to configure the interval for the BGP timely scan. Use the no or default form of this command to restore the default setting. bgp scan-time time no bgp scan-time

	default bgp scan-time	
Parameter Description	Parameter	Description
	<i>time</i>	Interval of the timely scan, in the range from 5 to 60 in the unit of seconds
Defaults	The default is 60.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, or BGP Scope configuration mode.	
Usage Guide	This command is used to configure the interval for the BGP timely scan; it takes effect when bgp scan-rib enable is configured.	
Configuration Examples	The following example configures the interval for the BGP timely scan.	
	FS(config-router)# bgp scan-time 30	
Related Commands	Command	Description
	bgp scan-rib enable	Enables timely scan of the routing table by BGP.
Platform Description	None	

5.47 bgp tcp-source-check disable

	Use this command to configure BGP's TCP source check function. Use no or default form of this command to disable this function.	
	bgp tcp-source-check disable	
	no bgp tcp-source-check disable	
	default bgp tcp-source-check disable	
Parameter Description	Parameter	Description
	-	-
Defaults	This function is enabled by default.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	After TCP source check function is disabled, all TCP connection requests will be received. After TCP connection is established, if no neighbor peer is configured on the local device, Notification packet will be send to refuse the BGP connection.	
Configuration Examples	The following example configures BGP's TCP source check function.	
	FS(config)# router bgp 65000	

	FS(config-router)# bgp tcp-source-check disable	
Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.
Platform	N/A	
Description		

5.48 bgp timer accuracy-control

	Use this command to configure BGP's internal timer accuracy control. Use no or default form of this command to restore the default setting.	
	bgp timer accuracy-control	
	no bgp timer accuracy-control	
	default bgp timer accuracy-control	
Parameter Description	Parameter	Description
	-	-
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode	
Usage Guide	By default, a deviation from the given time will occur on the BGP protocol's timer to prevent concurrent overtime of many timers. You can use this command to configure BGP protocol's timer to strictly implement the given time. It is recommended disabling this function unless necessary.	
Configuration Examples	The following example configures BGP's internal timer accuracy control. FS(config)# router bgp 65000 FS(config-router)# bgp timer accuracy-control	
Configuration Examples	Command	Description
	router bgp	Enables BGP protocol.
Platform	N/A	
Description		

5.49 bgp update-delay

	Use this command to set the maximum delay time of the BGP Speaker before sending the first updating information to neighbors. The no or default form of the command restores it to the default value. During the BGP

	graceful-restart, this command is used to update the delay time. bgp update-delay delay-time no bgp update-delay default bgp update-delay	
Parameter Description	Parameter	Description
	<i>delay-time</i>	Maximum delay time of the BGP Speaker before sending its route updating information, in the range from 0 to 3600 in the unit of seconds, 120 seconds by default. For BGP graceful-restart, it is the maximum time of waiting to receive the EOR message of all neighbors, in the range from 1 to 3600 in the unit of seconds.
Defaults	The default is 120.	
Command Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	With the BGP starting up, it first waits some time to connect with its neighbors, and then sends the updating message to these neighbors. After connecting with neighbors, the BGP does not send the updating message to them immediately, but waits some time to receive the updating routing message from all neighbors and then performs routing optimization calculation and finally advertises the route updating message to its neighbors, which improves the convergence time and reduces the calculation consumption. If the software sends the route updating information to its neighbors immediately, it may send the information again when it receives more optimized routes from other neighbors. The bgp update-delay command is used to adjust the initial waiting time of the software, which is the maximum time, from establishing the connection with the first neighbor to performing the routing optimization calculation and sending the route advertisement. When the BGP graceful-restart is enabled, this command is also used to set the maximum waiting time to receive EOR messages from all neighbors. You can increase this value if there are many neighbors or the routing information of the neighbors is huge. If the number of neighbors is 100 and the average amount of routes is 5000, the update sending time that each neighbor completes all the routing is 1 second, then the update of all the routing needs 100 seconds; if the number of neighbors increases to 200, the Update Delay time can be set to 240 seconds, ensuring that all the routing can be updated with the Update Delay period. The specific time is also related to data transmission rate.	
Configuration Examples	The following example sets the update-delay time to 200 seconds. <pre> FS(config)# router bgp 500 FS(config-router)# bgp graceful-restart FS(config-router)# bgp update-delay 200 </pre>	
Related Commands	Command	Description
	bgp graceful-restart	Enables the BGP graceful-restart.
Platform Description	None	

5.50 clear bgp all

	Use this command to reset all BGP address-families. The content to be reset depends on the further parameters . clear bgp all [as number] [soft] [in out]	
Parameter Description	Parameter	Description
	<i>none parameter</i>	Resets peer sessions in all address-families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
	in	Resets the received routing information.
	out	Resets the redistributed routing information.
	soft	Soft-resets all routing information received/sent from/to the specified peer.
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to reset sessions of all supported address-families, including the vrf session in every address-family.	
Configuration Examples	N/A	
Related Commands	Command	Description
	clear bgp ipv4 unicast	Resets the IPv4 unicast address-family.
Platform Description	None	

5.51 clear bgp all peer-group

	Use this command to reset BGP's specific peer group. The reset content is determined by further parameters.	
	clear bgp all peer-group <i>peer-group-name</i> [soft] [in out]	
Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Resets a specific peer group.
	in	Resets received route information.
	out	Resets allocated route information.

	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	This command will reset replies of all supported address families, including reply connection included in vrf in each address family.	
Configuration Examples	-	
Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.
Platform Description	-	

5.52 clear bgp all update-group

	Use this command to reset sessions of all members in an update-group. clear bgp all update-group [<i>update-group-index</i> <i>peer-address</i>] [soft] [in out]	
Parameter Description	Parameter	Description
	<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
	<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
	-	Resets BGP sessions directly if no option is carried.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets sent and received routing information.
	soft in	Soft-resets received routing information.
	soft out	Soft-resets distributed routing information.
Command Mode	Privileged EXEC mode	
Default Level	14	

Usage Guide	This command is used to reset BGP sessions of all members in an update-group.
Configuration Example	The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 belongs. <pre>FS# clear bgp all update-group 1.1.1.1 in</pre>

5.53 clear bgp ipv4 unicast

	Use this command to reset BGP IPv4 unicast address families. The reset content is determined by further parameters.	
	clear bgp ipv4 unicast [<i>vrf vrf-name</i>] { * <i>as-number</i> <i>peer-address</i> } [<i>soft</i>] [<i>in</i> <i>out</i>]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	*	Resets all peer group sessions under address families.
	<i>as-number</i>	Resets sessions with all members in the specified AS.
	<i>peer-address</i>	Resets sessions with the specified peer.
	<i>in</i>	Resets received route information.
	<i>out</i>	Resets allocated route information.
	<i>soft</i>	Soft-resets received and sent route information.
	<i>soft in</i>	Soft-resets received route information.
	<i>soft out</i>	Soft-resets allocated route information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is the same as clear ip bgp in terms of the function and parameters.	
Configuration Examples	N/A	
Configuration Examples	Command	Description
	N/A	N/A
Platform Description	N/A	

5.54 clear bgp ipv4 unicast dampening

	Use this command to clear the flap information and disable route dampening. clear bgp ipv4 unicast [vrf vrf-name] dampening [ip-address [mask]]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	-	Clears the flap information of all routes.
	<i>address</i>	IP address
	<i>mask</i>	Mask
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the BGP route dampening information and release suppressed routes. This command can be used to restart the BGP route dampening.	
Configuration Examples	The following example clears the flap information and disables route dampening. FS# clear ip bgp dampening 192.168.0.0 255.255.0.0	
Related Commands	Command	Description
	show ip bgp dampening dampened-paths	Displays the suppressed routing information.
	bgp dampening	Enables the route dampening and sets the dampening parameters.
Platform Description	None	

5.55 clear bgp ipv4 unicast external

	Use this command to reset all EBGp connections. clear bgp ipv4 unicast [vrf vrf-name] external [soft] [in out]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	in	Resets received route information.
	out	Resets allocated route information.
	soft	Soft-resets all routing information received/sent from/to the specified peer.
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	This command is used to reset the specified external BGP connection.	
Configuration Examples	The following example resets all EBGp connections. FS# clear bgp ipv4 unicast external in	
Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp neighbors	Displays the neighbor information.
Platform Description	None	

5.56 clear bgp ipv4 unicast flap-statistics

	Use this command to clear the route flap information. clear bgp ipv4 unicast [vrf vrf-name] flap-statistics [address [mask]]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	-	Clears all route flap information
	<i>address</i>	IP address
	<i>mask</i>	Mask
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can be used only to clear the statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the clear ip bgp dampening command.	
Configuration Examples	The following example clears the route flap information. FS# clear bgp ipv4 unicast flap-statistics	
Related Commands	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.57 clear bgp ipv4 unicast peer-group

	Use this command to reset the session with all members in the peer group. clear bgp ipv4 unicast [vrf vrf-name] peer-group peer-group-name [soft] [in out]	

Parameter Description	Parameter	Description
	vrf-name	VRF name
	peer-group-name	Name of the peer group
	in	Resets received route information.
	out	Resets allocated route information.
	soft	Soft-resets all routing information received/sent from/to the specified peer.
	soft in	Soft-resets for the received routing information.
	soft out	Soft-resets the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command resets the BGP session with all members in the peer group.	
Configuration Examples	The following example resets the session with all members in the peer group. FS# clear bgp ipv4 unicast peer-group my-group in	
Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.58 clear bgp ipv4 unicast table-map

	Use this command to update the table-map setting under the IPv4 unicast address family of BGP.	
	clear bgp ipv4 unicast [vrf vrf-name] table-map	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	Re-apply table-map setting and update allocated core route table information.	
Configuration Examples	-	

Parameter Description	Command	Description
	clear ip bgp	Resets BGP's IPv4 unicast address families.
Platform Description	-	

5.59 clear bgp ipv4 unicast update-group

Use this command to reset sessions of all members in an update-group in the IPv4 unicast address family.

clear bgp ipv4 unicast [**vrf** *vrf-name*] **update-group** [*update-group-index* | *peer-address*] [**soft**] [**in** | **out**]

Parameter Description	Parameter	Description
	<i>vrf-name</i>	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
	<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
	<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
	-	Resets BGP sessions directly if no option is carried.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets sent and received routing information.
	soft in	Soft-resets received routing information.
	soft out	Soft-resets distributed routing information.

Command Mode Privileged EXEC mode

Default Level 14

Usage Guide This command is used to reset BGP sessions of all members in an update-group in the IPv4 unicast address family.

Configuration Example The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 in the IPv4 unicast address family belongs.

```
FS# clear bgp ipv4 unicast update-group 1.1.1.1 in
```

5.60 clear bgp ipv6 unicast

	Use this command to reset BGP's IPv6 unicast address families.
	clear bgp ipv6 unicast [vrf <i>vrf-name</i>] { * <i>as-number</i> <i>peer-address</i> } [soft] [in out]

Parameter Description	Parameter	Description
	vrf-name	VRF name
	*	Resets all peer group sessions under address families.
	as-number	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
	peer-address	Resets sessions with the specified peer.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	The function is similar with clear bgp ipv4 unicast , but applies to different address families.	
Configuration Examples	-	
Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.
Platform Description	-	

5.61 clear bgp ipv6 unicast dampening

	Use this command to clear flap information and disable route dampening.	
	clear bgp ipv6 unicast [vrf vrf-name] dampening [ip-address [mask]]	
Parameter Description	Parameter	Description
	vrf-name	VRF name
	-	Clears all routes' flap information.

	<i>ip-address</i>	IP address
	<i>mask</i>	Mask code
Command Mode	Privileged EXEC mode	
Usage Guide	You can use this command to clear BGP's route flap information and disable route dampening. The command can restart BGP's route flap.	
Configuration Examples	The following example clears flap information and disables route dampening.	
Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
Platform Description	-	

5.62 clear bgp ipv6 unicast external

	Use this command to reset all EBGp connection of IPv6 unicast address families.	
	clear bgp ipv6 unicast [vrf vrf-name] external [soft] [in out]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	You can use this command to reset all the specified external BGP connection.	
Configuration Examples	The following example resets all EBGp connection of IPv6 unicast address families.	
	FS# clear bgp ipv6 unicast external in	

Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp neighbors	Displays BGP neighbors' information.
Platform Description	-	

5.63 clear bgp ipv6 unicast flap-statistics

	Use this command to clear IPv6 unicast address families' route flap statistics.	
	clear bgp ipv6 unicast [<i>vrf vrf-name</i>] flap-statistics [<i>address</i> [<i>mask</i>]]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	-	Clears all route information's flap information.
	<i>address</i>	IP address
	<i>mask</i>	Mask code
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the clear bgp ipv4 unicast dampening command.	
Configuration Examples	The following example clears IPv6 unicast address families' route flap statistics. FS# clear bgp ipv6 unicast flap-statistics	
Configuration Examples	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays BGP route entries.
Platform Description	-	

5.64 clear bgp ipv6 unicast peer-group

	Use this command to reset sessions with all members in the peer group.	
	clear bgp ipv6 unicast [vrf <i>vrf-name</i>] peer-group <i>peer-group-name</i> [soft] [in out]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	<i>peer-group-name</i>	Peer group name
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to reset BGP sessions with all members in the peer group.	
Configuration Examples	The following example resets sessions with all members in the peer group.	
	FS# clear bgp ipv6 unicast peer-group my-group in	
Configuration Examples	Command	Description
	clear ip bgp	Resets BGP sessions.
	show ip bgp	Displays BGP route entries.
Platform Description	-	

5.65 clear bgp ipv6 unicast table-map

	Use this command to update the table-map setting under the IPv6 unicast address family of BGP.	
	clear bgp ipv6 unicast [vrf <i>vrf-name</i>] table-map	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name

Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	-	
Configuration Examples	-	
Configuration Examples	Command	Description
	clear ip bgp	Resets BGP's IPv4 unicast address families.
Platform Description	-	

5.66 clear bgp ipv6 unicast update-group

	Use this command to reset sessions of all members in an update-group in the IPv6 unicast address family. clear bgp ipv6 unicast [vrf <i>vrf-name</i>] update-group [<i>update-group-index</i> <i>neighbor-address</i>] [soft] [in out]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
	<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
	<i>neighbor-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
	-	Resets BGP sessions directly if no option is carried.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets sent and received routing information.
	soft in	Soft-resets received routing information.
	soft out	Soft-resets distributed routing information.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	This command is used to reset BGP sessions of all members in an update-group in the IPv6 unicast address family.	

Configuration Example	The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1111::1111 in the IPv6 unicast address family belongs. <pre>FS# clear bgp ipv6 unicast update-group 1111::1111 in</pre>

5.67 clear bgp l2vpn evpn

	Use this command to reset BGP EVPN address families.	
	clear bgp l2vpn evpn { * <i>as-number</i> <i>neighbor-address</i> } [soft] [in out]	
Parameter Description	Parameter	Description
	*	Resets all peer group sessions under address families.
	<i>as-number</i>	Resets sessions with all members in the specified AS. In 10.4(3) or a later version, adds support for 4-byte AS numbers. The new AS number ranges from 1 to 4294967295, or 1 and 65535.65535 in the dotted mode.
	<i>neighbor-address</i>	Resets sessions with the specified peer.
	in	Resets received route information.
	out	Resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	The function is similar with clear bgp ipv4 unicast , but applies to different address families.	
Configuration Examples	-	
Configuration Examples	Command	Description
	clear bgp ipv4 unicast	Resets BGP's IPv4 unicast address families.
Platform Description	-	

5.68 clear bgp l2vpn evpn dampening

	Use this command to clear flap information and disable route dampening.	
	clear bgp l2vpn evpn dampening	
Parameter Description	Parameter	Description
	N/A	
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	You can use this command to clear BGP's route flap information and relieve damped routes. The command can restart BGP's route flap.	
Configuration Examples	The following example clears flap information and disables route dampening.	
	FS# clear bgp l2vpn evpn dampening	

Platform N/A

Description

5.69 clear bgp l2vpn evpn external

	Use this command to reset all EBGp connection of BGP EVPN address families.	
	clear bgp l2vpn evpn external [soft] [in out]	
Parameter Description	Parameter	Description
	in	Resets received route information.
	out	Resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	You can use this command to reset all the specified external BGP connection.	
Configuration	The following example resets all EBGp connection of L2VPN EVPN address families.	

Examples	FS# clear bgp l2vpn evpn external in
Platform	N/A
Description	

5.70 clear bgp l2vpn evpn flap-statistics

	Use this command to clear BGP EVPN address families' route flap statistics.	
	clear bgp l2vpn evpn flap-statistics	
Parameter Description	Parameter	Description
	N/A	
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can only clear statistics of routes that are not damped and will not relieve damped routes. To clear statistics of all route information and relieve damped routes, use the clear bgp l2vpn evpn dampening command.	
Configuration Examples	The following example clears L2VPN EVPN address families' route flap statistics. FS# clear bgp l2vpn evpn flap-statistics	
Platform	N/A	
Description		

5.71 clear bgp l2vpn evpn peer-group

	Use this command to reset sessions of all members in the peer group.	
	clear bgp l2vpn evpn peer-group <i>peer-group-name</i> [soft] [in out]	
Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Peer group name
	in	Resets received route information.
	out	Resets allocated route information.
	soft	Soft-resets received and sent route information.
	soft in	Soft-resets received route information.
	soft out	Soft-resets allocated route information.
Defaults	N/A	

Command Mode	Privileged EXEC mode
Usage Guide	Use this command to reset BGP sessions of all members in the peer group.
Configuration Examples	The following example displays that the L2VPN EVPN address family soft-resets received route information of all members in the peer group my-group. <pre>FS# clear bgp l2vpn evpn peer-group my-group in</pre>
Platform Description	N/A

5.72 clear bgp l2vpn evpn update-group

Use this command to reset sessions of all members in an update-group of L2VPN EVPN address family. clear bgp l2vpn evpn update-group [<i>update-group-index</i> <i>peer-address</i>] [soft] [in out]		
Parameter Description	Parameter	Description
	<i>update-group-index</i>	Specifies the index of an update-group, in which the sessions of members need to be reset.
	<i>peer-address</i>	Specifies the update-group, to which a peer whose session needs to be reset belongs.
	-	Resets BGP sessions directly if no option is carried.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets sent and received routing information.
	soft in	Soft-resets received routing information.
	soft out	Soft-resets distributed routing information.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	This command is used to reset BGP sessions of all members in an update-group of L2VPN EVPN address family.	
Configuration Example	The following example resets routing information received by all peers in an update group of L2VPN EVPN address family to which the peer with the IP address of 1.1.1.1 belongs. <pre>FS# clear bgp l2vpn evpn update-group 1.1.1.1 in</pre>	

5.73 clear evpn conflict mac

	Use this command to clear MAC information and other statistics of conflicts occurring in EVPN. clear evpn conflict mac [<i>vni-id</i>]	
Parameter Description	Parameter	Description
	<i>vni-id</i>	Clears MAC information and other statistics of conflicts occurring on a specified L2VNI.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	This command is used to clear conflict MAC information and re-advertise the EVPN routes corresponding to the conflict MAC.	
Configuration Example	The following example clears all conflict MAC information. FS# clear evpn conflict mac	

5.74 clear ip bgp

	Use this command to reset the BGP session. clear ip bgp [<i>vrf vrf-name</i>] { * <i>as-number</i> <i>peer-address</i> } [<i>soft</i>] [<i>in</i> <i>out</i>]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	*	Resets all the current BGP sessions and the OVERFLOW status of BGP ipv4 unicast address family.
	<i>address</i>	Resets the BGP session with the specified peer.
	<i>as number</i>	Resets sessions with all members in the specified AS. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new range of the new AS notation is from 1 to 4294967295, represented as 1 to 65535.65535 in dot mode.
	<i>in</i>	Reset the received routing information.
	<i>out</i>	Reset the distributed routing information.
	<i>soft</i>	Soft-reset all routing information received/sent from/to the specified peer
	<i>soft in</i>	Soft-reset the received routing information.
	<i>soft out</i>	Soft-reset the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	At any time, once the routing policy or BGP configuration changes, an effective way must be available to implement the new routing policy or configuration. Traditional measure is to close the BGP connection and establish a new one. This product supports implementing a new routing strategy without closing the BGP session connection by soft-resetting BGP. For the peer that does not support the route refresh function, you may run the neighbor soft-reconfiguration inbound command to keep a copy of original routing information of every specified BGP peer on the local BGP speaker. This will consume some resources. You can use the show ip bgp neighbors command to see whether the BGP peer supports the route refresh function. If it is supported, you need not to execute the neighbor soft-reconfiguration inbound command when the inbound routing strategy changes.  All connected BGP routers must support the route refresh function to execute this command. This product supports the route refresh function.	
Configuration Examples	The following example resets the BGP session. <pre>FS# clear bgp ipv4 unicast *</pre>	
Related Commands	Command	Description
	neighbor soft-reconfiguration inbound	(Optional) Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.75 clear ip bgp dampening

	Use this command to clear the dampening information and disable route dampening. <pre>clear ip bgp [vrf vrf-name] dampening [ip-address [mask]]</pre>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	<i>address</i>	IP address
	<i>mask</i>	Mask
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the BGP route flap information and disable route dampening. This command can be used to restart BGP route dampening.	
Configuration Examples	The following example clears the dampening information and disables route dampening. <pre>FS# clear ip bgp dampening 192.168.0.0 255.255.0.0</pre>	

Related Commands	Command	Description
	show ip bgp dampening dampened-paths	Displays the suppressed routing information.
	bgp dampening	Enables the route dampening function and sets dampening parameters.
Platform Description	None	

5.76 clear ip bgp external

	Use this command to reset all EBGp connections. clear ip bgp [vrf vrf-name] external [soft] [in out]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	in	Reset the received routing information.
	out	Reset the distributed routing information.
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to reset the specified external BGP connection.	
Configuration Examples	The following example resets all EBGp connections. FS# clear ip bgp external in	
Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp neighbors	Displays the neighbor information.
Platform Description	None	

5.77 clear ip bgp flap-statistics

	Use this command to clear the routes vibration statistics of the IPv4 unicast address family. clear ip bgp [vrf vrf-name] flap-statistics [ip-address [mask]]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
	<i>address</i>	IP address
	<i>Mask</i>	Mask

Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command can be used only to clear statistics of unsuppressed routes. It does not release the suppressed routes. To clear all route statistics and release the suppressed routes, run the clear ip bgp dampening command.	
Configuration Examples	The following example clears the routes vibration statistics of the IPv4 unicast address family. FS# clear ip bgp flap-statistics	
Related Commands	Command	Description
	bgp dampening	Enables the route dampening function and sets dampening parameters.
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.78 clear ip bgp peer-group

	Use this command to reset the session with all members in the peer group. clear ip bgp [vrf vrf-name] peer-group peer-group-name [soft] [in out]	
Parameter Description	Parameter	Description
	vrf-name	VRF name.
	peer-group-name	Name of the peer group
	in	Reset the received routing information.
	out	Reset the distributed routing information.
	soft	Soft-resets all routing information received/sent from/to the specified peer
	soft in	Soft-resets the received routing information.
	soft out	Soft-resets the distributed routing information.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command resets the BGP session with all members in the peer group.	
Configuration Examples	The following example resets the session with all members in the peer group. FS# clear ip bgp peer-group my-group in	
Related Commands	Command	Description
	clear ip bgp	Resets the BGP session.
	show ip bgp	Displays the BGP route entry.
Platform	None	

Description	

5.79 clear ip bgp table-map

	Use this command to update the table-map's route information applied by IPv4 unicast address family. clear ip bgp [vrf vrf-name] table-map	
Parameter	Parameter	Description
Description	vrf-name	vrf name
Defaults	N/A	
Command		
Mode	Privileged EXEC mode	
Usage Guide	This command is used to update the route information of the applied table-map.	
Configuration	The following example updates the table-map's route information applied by IPv4 unicast address family.	
Examples	FS# clear ip bgp table-map	
Related	Command	Description
Commands	clear ip bgp	Resets the BGP session.
	show ip bgp	Displays the BGP route entry.
Platform		
Description	None	

5.80 clear ip bgp update-group

	Use this command to reset sessions of all members in an update-group in the IPv4 unicast address family. clear ip bgp [vrf vrf-name] update-group [update-group-index neighbor-address] [soft] [in out]	
Parameter	Parameter	Description
Description		
	vrf-name	Specifies the name of a VRF instance. A global VRF instance is used if no VRF instance name is entered.
	update-group-index	Specifies the index of an update-group, in which the sessions of members need to be reset.
	neighbor-address	Specifies the update-group, to which a peer whose session needs to be reset belongs.
	-	Resets BGP sessions directly if no option is carried.
	in	Resets received routing information.
	out	Resets distributed routing information.
	soft	Soft-resets sent and received routing information.
	soft in	Soft-resets received routing information.
	soft out	Soft-resets distributed routing information.

Command Mode	Privileged EXEC mode
Default Level	14
Usage Guide	This command is used to reset BGP sessions of all members in an update-group in the IPv4 unicast address family.
Configuration Example	The following example resets routing information received by all peers in an update group to which the peer with the IP address of 1.1.1.1 in the IPv4 unicast address family belongs. <pre>FS# clear ip bgp update-group 1.1.1.1 in</pre>

5.81 default-information originate

	Use this command to enable BGP to distribute the default route. Use the no form of this command to restore the default setting. default-information originate [no] default-information originate default default-information originate	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, BGP IPv4 VRF configuration mode, BGP IPv6 VRF configuration mode	
Usage Guide	This command is used to control whether the redistributed default route is effective, and this command needs to be configured together with the redistribute command. It takes effect only when a default route exists in the redistributed route. This command is similar to the network command. The difference is that in the process of configuring the former, the redistribute command must be configured explicitly to redistribute the default route, only in this case, the redistributed default route is effective. For the later command, the IGP must have the default route.	
Configuration Examples	The following example enables BGP to distribute the default route.	
	FS(config-router)# default-information originate	
Related Commands	Command	Description
	network	Configures routes to be advertised.
	redistribute	Redistributes routes of other protocol.
Platform Description	None	

5.82 default-metric

	Use this command to set the metric for route redistribution. Use the no or default form of this command to restore the default setting. default-metric number no default-metric default default-metric	
Parameter	Parameter	Description
Description	<i>number</i>	Metric number, in the range from 1 to 4294967295
Defaults	No metric is set by default.	
Command Mode	BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command sets the metric of routes to be redistributed for integrity.  The metric set by the command cannot cover that set by the redistribute metric command. The value is 0 when the default metric applies to redistributed connected routes.	
Configuration Examples	The following example sets the metric for route redistribution. <pre>FS(config-router)# default-metric 45</pre>	
Related Commands	Command	Description
	redistribute	Redistributes routes of other protocol.
Platform Description	None	

5.83 distance bgp

	Use this command to set different management distances for different types of BGP routes. Use the no or default form of this command to restore the default setting. distance bgp external-distance internal-distance local-distance no distance bgp default distance bgp	
Parameter Description	Parameter	Description
	<i>external-distance</i>	Route management distance learned from EBGp peers, in the range from 1 to 255
	<i>internal-distance</i>	Route management distance learned from IBGP peers, in the range from 1 to 255
	<i>local-distance</i>	Specifies the management distance of route learned from peers. However, the optimal one can be learned from the IGP. In general, these routes are indicated by the Network Backdoor command. The value is in the range from 1 to 255
Defaults	The parameter defaults are as follows: <i>external-distance - 20</i>	

	<i>internal-distance - 200</i> <i>local-distance - 200</i>	
Command Mode	BGP configuration mode or BGP Scope configuration mode.	
Usage Guide	It is not recommended to change the management distance of the BGP route. If it is necessary, observe the following points: ● The management distance of "external-distance" must be shorter than those of other IGP routing protocols (such as OSPF and RIP); ● The internal-distance and local-distance should have longer management distances than other IGP routing protocols.	
Configuration Examples	The following example sets different management distances for different types of BGP routes. <pre>FS(config-router)# distance bgp 20 20 200</pre>	
Related Commands	Command	Description
	neighbor soft-reconfiguration inbound	Restarts the BGP session and reserves the unchanged route information sent by the BGP peer (group).
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.84 evpn

	Use this command to enter EVPN configuration mode. Use the no or restore form of this command to restore the default settings. <pre>evpn no evpn default evpn</pre>	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, the EVPN configuration mode is disabled.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enter EVPN configuration mode. Use the exit command to exit the EVPN configuration mode	
Configuration Examples	The following example enters EVPN configuration mode. <pre>FS(config)# evpn</pre>	
Platform Description	N/A	

5.85 exit-address-family

	Use this command to exit BGP address-family configuration mode. exit-address-family	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	BGP address-family configuration mode	
Usage Guide	This command can be used to exit from various address-family modes of BGP to BGP configuration mode.	
Configuration Examples	The following example exits the BGP address-family configuration mode. FS(config-router-af)#exit-address-family	
Related Commands	Command	Description
	address-family ipv4	Enters IPv4 address family configuration mode.
Platform Description	None	

5.86 export map(EVPN VNI)

	Use this command to configure the route map for exporting the extended community attribute of EVPN routes from the local device to the remote device. Use the no form of this command to delete the route map for exporting the extended community attribute of EVPN routes from the local device to the remote device. Use the default form of this command to restore the default settings. export map <i>route-map-name</i>	
	no export map	
	default export map	
Parameter	Parameter	Description
Description	<i>route-map-name</i>	Name of the route map
Defaults	No route map is configured for exporting the extended community attribute by default.	
Command Mode	EVPN VNI configuration mode.	
Default Level	14	
Usage Guide	This command is used to modify the extended community attribute advertised by a type 5 route converted from a local EVPN route or IP route. This command supports only one route map, and the old configuration is overwritten by the new configuration.	

Configuration Examples	The following example configures a route map for exporting the extended community attribute associated with map1 on VNI 1. <pre>FS(config)# evpn FS(config-evpn)# vni 1 FS(config-evpn-vni)# export map map1</pre>
Verification	Run the show running-config command to display the configurations.

5.87 import map(EVPN VNI)

	Use this command to configure the route map for importing the remote EVPN routes to the local VNI instance. Use the no form of this command to delete the route map for importing the remote EVPN routes to the local VNI instance. Use the default form of this command to restore the default settings. import map <i>routemap-name</i>	
	no import map	
	default import map	
Parameter	Parameter	Description
Description	<i>routemap-name</i>	Name of the route map
Defaults	No route map is configured for importing the remote EVPN routes to the local VNI instance by default.	
Command Mode	EVPN VNI configuration mode.	
Default Level	14	
Usage Guide	This command is used to filter the remote EVPN routes to be imported to the local VNI instance, or modify the attribute of the remote EVPN routes imported to the local VNI instance. This command supports only one route map, and the old configuration is overwritten by the new configuration.	
Configuration Examples	The following example configures the route map map1 for importing the remote EVPN routes to the local VNI instance vni 1. FS(config)# evpn FS(config-evpn)# vni 1 FS(config-evpn-vni)# import map map1	
Verification	Run the show running-config command to display the configurations.	

5.88 maximum-paths

	Use this command to configure the number of equivalent paths of the EBGP/IBGP multipath load balancing function. Use the no form of this command to disable the EBGP/IBGP multipath load balancing function. Use the default form of this command to restore the default settings.

	maximum-paths { ebgp ibgp } number	
	no maximum-paths { ebgp ibgp }	
	default maximum-paths { ebgp ibgp }	
Parameter Description	Parameter	Description
	ebgp	Specifies the number of equivalent paths of the EBGp multipath load balancing function.
	ibgp	Specifies the number of equivalent paths of the IBGP multipath load balancing function.
	number	Indicates the maximum number of equivalent paths. The minimum value is 1, and the maximum value depends on the device capability. If the value is 1, the EBGp multipath load balancing function is disabled.
Defaults	Equivalence of multiple BGP paths is not supported by default.	
Command Mode	BGP configuration mode, BGP IPv4 Unicast address family configuration mode, BGP IPv6 Unicast address family configuration mode, and BGP Scope Global configuration mode	
Default Level	14	
Usage Guide	The maximum-paths ebgp command is also used to configure equivalence of confederation EBGp multiple paths and local inter-VRF import routes. IBGP and EBGp routes cannot form equivalent routes.	
Configuration Examples	The following example configures EBGp load balancing and sets the maximum number of equivalent routes to 2. <pre>FS(config)# router bgp 65530 FS(config-router)# maximum-paths ebgp 2</pre>	
Verification	Run the show running-config command to display the BGP configurations.	

5.89 maximum-prefix

	Use this command to limit the maximum number of prefixes in the routing database in the address family. Use the no or default form of this command to restore the default setting. maximum-prefix maximum no maximum-prefix default maximum-prefix	
Parameter Description	Parameter	Description
	<i>maximum</i>	The maximum number of prefixes in the routing database in the address family, in the range from 1 to 4294967295
Defaults	The maximum number is not limited by default.	
Command	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF	

Mode	configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	In a BGP address family, routing prefixes may be introduced through redistribution or learnt from neighbors, or other VRFs. Once routing prefixes in the BGP address family reaches the maximum number, this address family will enter to the overflow state. Use the show bgp { addressfamily all } summary command to display the state of routing database. It is necessary to reconfigure BGP for state clearing, or use the clear bgp { addressfamily all } * command to reset the address family.	
	 When the address family is overflow as the number of prefixes reaches the maximum number, you can adjust maximum-prefix.	
	 Maximum-prefix will not filter the routing information generated by the network and aggregate commands. IPv4 unicast routes can receive the routing prefix in the following conditions even in the Overflow state: The route information of the same routing prefix exists in the address database. One route that overwrites this prefix (except for the default route) exists in the address database and the next-hop of this route is different from that of the newly received routing prefix.	
Configuration Examples	The following example sets the maximum number of prefixes in the BGP routing database in the ipv4 multicast address family. <pre>FS(config)# router bgp 65000 FS(config-router)# address-family ipv4 multicast FS(config-router-af)# maximum-prefix 65535</pre>	
Related Commands	Command	Description
	clear bgp all	Resets BGP's all address families.
	clear bgp ipv4 mdt	Resets BGP's ipv4 mdt address families.
	clear bgp ipv4 unicast	Resets BGP's ipv4 unicast address families.
	clear bgp ipv6 unicast	Resets BGP's ipv6 unicast address families.
	clear bgp vpnv4 unicast	Resets BGP's vpnv4 unicast address families.
	show bgp all summary	Displays summary of BGP's all address families.
	show bgp ipv4 mdt summary	Displays summary of BGP's ipv4 mdt address families.
	show bgp ipv4 unicast summary	Displays summary of BGP's ipv4 unicast address families.
	show bgp ipv6 unicast summary	Displays summary of BGP's ipv6 unicast address families.
	show bgp vpnv4 summary	Displays summary of BGP's vpnv4 unicast address families.
Platform Description	N/A	

5.90 neighbor activate

	Use this command to activate the neighbor or peer group in the current address mode. Use the no or default form of this command to disable this function. neighbor {peer-address peer-group-name} activate no neighbor {peer-address peer-group-name} activate

	default neighbor { peer-address peer-group-name } activate	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 address or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	This function is enabled in IPv4 address family mode by default.	
Command Mode	BGP configuration mode, BGP IPv4/ IPv6 Unicast address family configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode, or BGP Scope configuration mode.	
Usage Guide	The function is enabled by default for IPv4 address families. You need to set this command in other address-family configuration modes for exchanging routes.	
Configuration Examples	The following example activates the neighbor or peer group in the current address mode.	
	FS(config)# router bgp 60	
	FS(config-router)# neighbor 10.0.0.1 remote-as 100	
	FS(config-router)# address-family vpnv4	
	FS(config-router-af)# neighbor 10.0.0.1 activate	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.91 neighbor advertisement-interval

	Use this command to set the time interval to send the BGP route update message. Use the no or default form of this command to restore the default setting. neighbor { peer-address peer-group-name } advertisement-interval seconds no neighbor { peer-address peer-group-name } advertisement-interval default neighbor { peer-address peer-group-name } advertisement-interval	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>seconds</i>	Time interval to send the route update message in the range from 0 to 600 seconds
Defaults	IBGP connection: 15 seconds EBGP connection: 30 seconds	
Command Mode	BGP configuration mode, BGP IPv4/ IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.	

Configuration Examples	The following example sets the time interval to send the BGP route update message.	
	<pre>FS(config)# router bgp 60 FS(config-router)# neighbor 10.0.0.1 remote-as 100 FS(config-router)# neighbor 10.0.0.1 advertisement-interval 10</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.92 neighbor allowas-in

	Use this command to allow the PE to receive messages with the same AS number as itself. Use the no or default form of this command to restore the default setting. <pre>neighbor {peer-address peer-group-name} allowas-in number no neighbor {peer-address peer-group-name} allowas-in default neighbor {peer-address peer-group-name} allowas-in</pre>	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>number</i>	Number of the AS number duplication in the range from 1 to 10, 3 by default
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	A typical application is spoke_hub mode. Execute this command on the PE to enable it to receive and then send the advertised address prefix. Configure two VRFs on the PE. One VRF receives the routes of all PEs and advertises them to the CE; the other VRF receives the routes advertised by the CE and advertises them to all PEs. This command applies to IBGP or EBGP peers.	
Configuration Examples	The following example allows the PE to receive messages with the same AS number as itself.	
	<pre>FS(config)# router bgp 60 FS(config-router)# neighbor 10.1.1.1 remote-as 100 FS(config-router)# address-family ipv4 vrf vpn1 FS(config-router-af)# neighbor 10.1.1.1 allowas-in</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.93 neighbor as-originate-interval

	Use this command to configure the interval that the device advertises local original BGP routes to the peer (group). Use the no or default form of this command to restore the default setting. neighbor { peer-address peer-group-name } as-origination-interval seconds no neighbor { peer-address peer-group-name } as-origination-interval default neighbor { peer-address peer-group-name } as-origination-interval	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer.
	<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.
	<i>seconds</i>	The interval at which the device advertises local original BGP routes to the peer (group), in the range from 1 to 65535 in the unit of seconds.
Defaults	The default interval is 1.	
Command Mode	BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family configuration mode/ BGP scope global configuration mode.	
Usage Guide	If you specify a peer group name in this command, the configuration takes effect on all members of the peer group.	
Configuration Examples	The following example configures the interval at which the device advertises local original BGP routes to the peer in the BGP IPv4 VRF address family configuration mode. <pre>FS(config)# router bgp 60 FS(config-router)# address-family ipv4 vrf vpn1 FS(config-router-af)# neighbor 10.0.0.1 remote-as 100 FS(config-router-af)# neighbor 10.0.0.1 as-origination-interval 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.94 neighbor default-originate

	Use this command to allow the BGP speaker to advertise the default route to the peer (group). Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} default-originate [route-map map-tag] no neighbor {peer-address peer-group-name} default-originate [route-map map-tag] default neighbor { peer-address peer-group-name } default-originate [route-map map-tag]	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters

	<i>map-tag</i>	Name of the route-map of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, or BGP Scope configuration mode	
Usage Guide	This command does not requires the default route but sends a default route whose next-hop address is the local address to neighbors. If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command. If you set the command for a member in the peer, this command will overwrite the settings on the peer group.	
Configuration Examples	The following example allows the BGP speaker to advertise the default route to the peer (group). <pre>FS(config)# router bgp 60 FS(config-router)# neighbor 10.1.1.1 remote-as 80 FS(config-router)# neighbor 10.1.1.1 default-originate</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.95 neighbor description

	Use this command to set a descriptive sentence for the specified peer (group). Use the no or default form of this command to restore the default setting. <pre>neighbor {peer-address peer-group-name} description text no neighbor {peer-address peer-group-name} description default neighbor { peer-address peer-group-name } description</pre>	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>text</i>	Descriptive text of the peer (group) of up to 80 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode and BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to add descriptive characters for the peer (group). This may help remember features and characteristics of the peer (group).	
Configuration Examples	The following example sets a descriptive sentence for the specified peer (group). <pre>FS(config)# router bgp 60 FS(config-router)# neighbor 10.1.1.1 remote-as 80</pre>	

	FS(config-router)# neighbor 10.1.1.1 description xyz.com	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform		
Description	None	

5.96 neighbor distribute-list

	Use this command to implement the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer. Use the no or default form of this command to restore the default setting. neighbor { peer-address peer-group-name } distribute-list { access-list-number } { in out } no neighbor { peer-address peer-group-name } distribute-list { access-list-number } { in out } default neighbor { peer-address peer-group-name } distribute-list { access-list-number access-list-name } { in out }	
Parameter Description	Parameter	Description
	peer address	IP address of the peer
	peer-group-name	Name of the peer group of up to 32 characters
	access-list-number	ACL number
	in	Specifies the ACL for filtering the incoming routes.
	out	Specifies the ACL for filtering the outgoing routes.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.	
Usage Guide	For in rule or out rule, this command cannot be used together with the neighbor prefix-list command. Only one of them can take effect.	
	If you have specified the BGP peer group, all members of the peer group will adopt the settings. If you set the neighbor distribute-list command for a member in the peer, this command will overwrite the settings on the peer group.	
	You can set different filtering policies in different address-family configuration modes to control routes.	
Configuration Examples	The following example implements the routing policy based on the ACL when receiving/sending route information from/to the specified BGP peer.	
	<pre>FS(config)# router bgp 60 FS(config-router)# neighbor 10.1.1.1 remote-as 80 FS(config-router)# neighbor 10.1.1.1 distribute-list bgp-filter in</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	ip access-list	Creates a standard IP ACL or extended IP ACL.
Platform	None	

Description	

5.97 neighbor ebgp-multihop

	Use this command to allow establishing BGP connection between EBGp peers that are not directly connected. Use the no or default form of this command to restore the default setting. <pre>neighbor {peer-address peer-group-name} ebgp-multihop [ttl] no neighbor {peer-address peer-group-name} ebgp-multihop [ttl] default neighbor { peer-address peer-group-name } ebgp-multihop [ttl]</pre>	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>ttl</i>	Maximum hops in the range 1 to 255
Defaults	The BGP connection is allowed between EBGp peers connected with each other directly by default. If "ebgp-multihop" is followed by no parameter, the ttl is 255.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	To prevent routing loop and dampening, non-default routes that can reach the peer must exist between EBGp peers between which the BGP connection can only be established via multiple hops. If the BGP peer group is specified, all members of the peer group adopt the settings. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example allows establishing BGP connection between EBGp peers that are not directly connected. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 remote-as 65100 FS(config-router)# neighbor 10.0.0.1 ebgp-multihop</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.98 neighbor fall-over bfd

	Use this command to enable BFD correlation with BGP. Use the no form or default form of this command to disable BFD correlation with BGP. <pre>neighbor { peer-address peer-group-name } fall-over bfd no neighbor { peer-address peer-group-name } fall-over bfd default neighbor { peer-address peer-group-name } fall-over bfd</pre>	
Parameter Description	Parameter	Description
	<i>peer address</i>	IPv4 or IPv6 address of the peer.
	<i>peer-group-name</i>	Name of the peer group, containing up to 32 characters.

Defaults	BFD correlation is disabled by default.	
Command Mode	BGP configuration mode / IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode/ Scope configuration mode	
Usage Guide	Before configuring BFD correlation, the BFD session parameters of the neighbor interface must be configured.	
Configuration Examples	The following example enables BFD correlation to detect the forwarding path between local and the neighbor 172.16.0.2. <pre>FS(config)# router bgp 45000 FS(config-router)# neighbor 172.16.0.2 remote-as 45001 FS(config-router)# neighbor 172.16.0.2 fall-over bfd</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.99 neighbor filter-list

	Use this command to enable route filtering when sending/receiving routing information to/from BGP peers. Use the no or default form of this command to restore the default setting. <pre>neighbor { peer-address peer-group-name } filter-list access-list-number { in out } no neighbor { peer-address peer-group-name } filter-list access-list-number { in out } default neighbor { peer-address peer-group-name } filter-list access-list-number { in out }</pre>	
Parameter Description	Parameter	Description
	peer address	IP address of the peer, IPv4 address or IPv6 address
	peer-group-name	Name of the peer group of up to 32 characters
	access-list-number	ACL number
	in	Applies as-path list on the received routing information.
	out	Applies as-path list on the distributed routing information.
Defaults	The function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.	
Usage Guide	If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the neighbor filter-list command is set for a member of the peer, the setting will overwrite the setting for the group. You can set different filter policies in different address-family configuration modes to control routes.	
Configuration Examples	The following example enables route filtering when sending/receiving routing information to/from BGP peers. <pre>FS(config)# ip as-path access-list 1 deny _123_ FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 remote-as 65100</pre>	

	FS(config-router)# neighbor 10.0.0.1 filter-list 1 out	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	ip as-path access-list	Creates an AS_PATH list.
	match as-path	Matches the AS_PATH list.
Platform Description	None	

5.100 neighbor local-as

	Use this command to configure the local AS number for the BGP peer, which could be used as its Remote AS to connect with local router. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} local-as as-number [no-prepend [replace-as [dual-as]]] no neighbor {peer-address peer-group-name} local-as default neighbor { peer-address peer-group-name } local-as	
Parameter Description	Parameter	Description
	<i>peer address</i>	IP address of the peer, IPv4 address or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>as-number</i>	Local AS number, in the range from 1 to 65535. In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.
	no-prepend	The AS-PATH of the routing information received from the peer does not depend on the Local AS. This option is disabled by default.
	replace-as	The AS-PATH of the routing information sent to the peer replaces the BGP AS with the Local AS. This option is disabled by default.
	dual-as	Uses BGP AS or Local AS to establish BGP connection with the device. This option is disabled by default.
Defaults	No Local AS is configured for the peer. If Local AS is configured, no option is configured by default. The peer could only use Local AS to establish BGP connection with local device, and adds Local AS into the AS-PATH of the received routing information, inserts Local AS to the corresponding AS-PATH before sending the routing information to the peer.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.	
Usage Guide	Local AS could be configured on the EBGp peer only, and if the attributes of the peer change, such as EBGp converts to IBGP or union EBGp, Local AS and corresponding options will be deleted. Local AS must be different from BGP AS and this peer's Remote AS and the union ID (if federation is configured). If you have specified the BGP peer group, all members of this peer group will adopt the settings of this command. You cannot set Local AS for the specified member of the peer group separately.	
Configuration	The following example configures the local AS number for the BGP peer.	

Examples	FS(config)# router bgp 65000	
	FS(config-router)# neighbor 10.0.0.1 remote-as 65100	
	FS(config-router)# neighbor 10.0.0.1 local-as 23	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	N/A	

5.101 neighbor maximum-prefix

	Use this command to limit the number of prefixes received from the specified BGP peer. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} maximum-prefix maximum [threshold] [warning-only] no neighbor {peer-address peer-group-name} maximum-prefix maximum default neighbor { peer-address peer-group-name } maximum-prefix maximum	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>maximum</i>	Upper limit of the number of the received route entries
	<i>threshold</i>	Percentage of the maximum when alarming.
	warning-only	Does not terminate the BGP connection when the route entries reach the upper limit but produce a log entry.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	The BGP connection will be torn down when the received routes exceeds the upper limit by default. To prevent tearing down the connection, set the "warning-only" to control that. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example limits the number of prefixes received from the specified BGP peer. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 maximum-prefix 1000</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.102 neighbor next-hop-self

	Use this command to set the next-hop of the route to the local BGP speaker while specifying the routes that the BGP peer redistributes. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} next-hop-self no neighbor {peer-address peer-group-name} next-hop-self default neighbor { peer-address peer-group-name } next-hop-self	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is mostly used in the non-full-mesh-type network, such as the Frame Relay and X.25, where the BGP speakers within the same subnet cannot completely be accessed mutually. If you have specified the BGP peer group, all members of the peer group will adopt the settings of the command.	
Configuration Examples	The following example sets the next-hop of the route to the local BGP speaker.	
	<pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 next-hop-self</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.103 neighbor next-hop-unchanged

	Use this command to maintain the next-hop when sending routes to the peer(group). Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} next-hop-unchanged no neighbor {peer-address peer-group-name} next-hop-unchanged default neighbor { peer-address peer-group-name } next-hop-unchanged	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	next-hop-unchanged	Maintains the next-hop while sending the routes to the peer(group).
Defaults	The next-hop will be changed by default when routes are sent to the EBGp peer.	
Command	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP L2VPN EVpn address	

Mode	family configuration mode or BGP Scope Global configuration mode.	
Usage Guide	This command is used to control to maintain the next-hop route transmitting between multi-hop EBGP peer sessions. This command cannot be configured on the route reflector. And for the client of the route reflector, if this function is enabled, the neighbor next-hop-self command cannot be used to change the next-hop of routes. This function is mainly applied to the cross-domain VPN. In the implementation with the Option C adopted, to reduce the complete connectivity between the PEs of the cross-domain CPN, a route reflector can be set in every autonomous domain to establish the Multihop MP-EBGP connection to implement the VPN route interaction. As the next-hop route is changed as itself while sending routes to the EBGP peer by default, PE stations of other autonomous domains will consider the final next-hop of the VPN route as the route reflector when receiving the VPN route at last, which will result in all cross-domains VPN flow going through the reflector. However, usually this is not the optimal forwarding path, and the requirement for the forwarding performance of the RR is higher. To avoid this condition, use the neighbor next-hop-unchanged command in the address-family VPNv4 configuration mode to maintain the next-hop of the VPNv4 route sent to the BGP peer when establishing the cross-domain Multihop MP-EBGP connection on the router reflector.	
Configuration Examples	The following example maintains the next-hop when sending routes to the peer (group). <pre>FS(config)# router bgp 60 FS(config-router)# address-family vpnv4 FS(config-router-af)# neighbor 10.1.1.1 next-hop-unchanged</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.104 neighbor password

	When the BGP connection with the BGP peer is established, use this command to enable TCP MD5 authentication and set the password. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} password [0 7]string no neighbor {peer-address peer-group-name} password default neighbor { peer-address peer-group-name } password	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	0	Displays the password with encryption.
	7	Displays the password without encryption.
	<i>string</i>	Password for MD5 authentication in the range from up to 80 characters
Defaults	The function is disabled by default	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	

Usage Guide	This command will enable MD5 authentication of the TCP. BGP peers must have the same password configured; otherwise, the neighbor relationship cannot be established. When this command is set, the local BGP speaker will re-establish the BGP connection with the BGP peer. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group. No matter in which mode, a neighbor has only one password, not one for every address family, .	
Configuration Examples	The following example enables TCP MD5 authentication and sets the password. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 password Red-Giant</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.105 neighbor peer-group (creating)

	Use this command to create a BGP peer group. Use the no or default form of this command to restore the default setting. <pre>neighbor peer-group-name peer-group no neighbor peer-group-name peer-group default neighbor peer-group-name peer-group</pre>	
Parameter Description	Parameter	Description
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	No BGP peer group is created.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF configuration mode or BGP Scope configuration mode.	
Usage Guide	If multiple BGP peers use the same update policy, the peers can be configured in the same peer group, so as to simplify the configuration and boost operation efficiency.	
Configuration Examples	The following example creates a BGP peer group. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor Red-Giant peer-group</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	neighbor peer-group (assigning members)	Configures the specified peer as the member of the BGP peer group.
	show ip bgp peer-group	Displays the information of the BGP peer.

Platform	
Description	None

5.106 neighbor peer-group (assigning members)

	Use this command to configure the specified peer as a member of the BGP peer group. Use the no or default form of this command to restore the default setting. neighbor peer-address peer-group peer-group-name no neighbor peer-address peer-group peer-group-name default neighbor peer-address peer-group peer-group-name	
Parameter Description	Parameter	Description
	peer-address	IP address of the peer, IPv4 or IPv6 address
	peer-group-name	Name of the peer group of up to 32 characters
Defaults	No peer exists in the peer group.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	Members of the peer group can adopt all configurations of the peer. It is allowed to configure an individual member of the peer group to replace the universal configuration for the peer group, but such separate configuration does not contain the configuration information that may affect the output update. In other words, every member in the peer group will always adopt the following configurations of the peer group: remote-as, update-source, local-as, reconnect-interval, times, advertisement-interval, default-originate, next-hop-self, remove-private-as, send-community, distribute-list out, filter-list out, prefix-list out, route-map out, unsuppress-map, route-reflector-client.  Do not place neighbors of different address families in the same peer group, or place IBGP and EBGP neighbors in the same peer group.	
Configuration Examples	The following example configures the specified peer as a member of the BGP peer group. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor Red-Giant peer-group FS(config-router)# neighbor 10.0.0.1 peer-group Red-Giant</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	neighbor peer-group (creating)	Creates the BGP peer group.
	show ip bgp peer-group	Displays the information of the BGP peer.
Platform Description	None	

5.107 neighbor prefix-list

	Use this command to implement the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} prefix-list prefix-list-name { in out } no neighbor {peer-address peer-group-name} prefix-list prefix-list-name { in out } default neighbor { peer-address peer-group-name } prefix-list prefix-list-name { in out }	
Parameter Description	Parameter	Description
	peer address	IP address of the peer, IPv4 or IPv6 address
	peer-group-name	Name of the peer group of up to 32 characters
	prefix-lis-name	Name of the prefix-list of up to 32 characters
	in	Applies the prefix list to the received routes.
	out	Applies the prefix list to the redistributed routes.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode or BGP Scope configuration mode.	
Usage Guide	For the "in" rule or "out" rule, this command cannot be used together with the neighbor distribute-list command. That is, only one of them takes effect. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If the neighbor prefix-list in command is set for a member of the peer, the setting will overwrite the setting for the group. You can set different filter policies in different address-family configuration modes to control routes.	
Configuration Examples	The following example implements the routing policy based on the prefix list to receive/transmit routes from/to the BGP peer. <pre>FS(config)# ip prefix-list bgp-filter deny 10.0.0.1/16 FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 prefix-list bgp-filter in</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	ip prefix-list	Creates the prefix lists.
Platform Description	None	

5.108 neighbor remote-as

	Use this command to configure the BGP peer (group). Use the no or default form of this command to restore the default setting. neighbor { peer-address peer-group-name } remote-as as-number

	no neighbor { peer-address peer-group-name } remote-as default neighbor { peer-address peer-group-name } remote-as	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>as-number</i>	BGP peer (group) autonomous system number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.
Defaults	No BGP peer is configured.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	If you have specified the BGP peer group, all members of the peer group will inherit the settings of the command.	
Configuration Examples	The following example configures the BGP peer (group).	
	<pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 remote-as 80</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
Platform Description	None	

5.109 neighbor remove-private-as

	Use this command to delete the private AS number recorded in the AS path attribute in the route sent to the specified EBGP peer. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} remove-private-as no neighbor {peer-address peer-group-name} remove-private-as default neighbor { peer-address peer-group-name } remove-private-as	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 address family configuration mode, or BGP IPv4 VRF configuration mode.	
Usage Guide	This command takes effect only on EBGP peers.	
	If the AS path contains the private AS number that is the AS number of the EBGP peer to be sent, the AS number is not deleted.	

	Private AS number range: 64512 - 65535	
Configuration Examples	The following example deletes the private AS number recorded in the AS path attribute in the route sent to the specified EBGp peer <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 remove-private-as</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.110 neighbor route-map

	Use this command to enable route match for the received/sent routes. Use the no or default form of this command to disable this function. <pre>neighbor { peer-address peer-group-name } route-map map-tag { in out } no neighbor { peer-address peer-group-name } route-map map-tag { in out } default neighbor { peer-address peer-group-name } route-map map-tag { in out }</pre>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>map-tag</i>	Name of the match rule
	in	Applies the rule to the incoming routes.
	out	Applies the rule to the outgoing routes.
Defaults	N/A	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command can be used to filter the incoming and outgoing routes for different neighbors by using different incoming/outgoing rules, purifying and controlling routes. You can set different filter policies in different address-family configuration modes to control routes.	
Configuration Examples	The following example enables route match for the received/sent routes. <pre>FS(config-router)# neighbor 10.0.0.1 route-map map-tag in</pre>	
Related Commands	Command	Description
	neighbor soft-reconfiguration inbound	Stores the routing information sent from the BGP peer.
	show ip bgp	Displays the BGP route entry.
Platform Description	None	

5.111 neighbor route-reflector-client

	Use this command to configure the local device as the route reflector and specifies its client. Use the no or default form of this command to restore the default setting. neighbor peer-address route-reflector-client no neighbor peer-address route-reflector-client default neighbor { peer-address peer-group-name } route-reflector-client	
Parameter	Parameter	Description
Description	peer-address	IP address of the peer, IPv4 or IPv6 address
	peer-group-name	Name of the peer. The name cannot exceed 32 characters.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode or BGP Scope configuration mode.	
Usage Guide	By default, all IBGP speakers in the autonomous system must establish neighbor relationship with each other. The BGP speaker does not forward the routes learned from an IBGP peer to other IBGP peers to avoid route loop. This command can be used to set route reflector, so that there is no need for all IBGP speakers to establish full neighboring relationship between each other. This will allow the route reflector to forward learned IBGP routes to other IBGP peers.	
Configuration Examples	The following example configures the local device as the route reflector and specifies its client. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 route-reflector-client</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	bgp cluster-id	Configures the cluster ID of the route reflectors.
	bgp client-to-client reflection	Enables the route reflection between clients
Platform Description	None	

5.112 neighbor send-community

	Use this command to transmit community attributes to the specified BGP neighbor. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} send-community [both standard extended] no neighbor {peer-address peer-group-name} send-community [both standard extended] default neighbor { peer-address peer-group-name } send-community [both standard extended]

	Parameter	Description
Parameter Description	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	both	Transmits both standard and extended communities.
	standard	Transmits the standard community only.
	extended	Transmits the extended community only.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode, BGP scope configuration mode	
Usage Guide	This command transmits the community to the neighbor or neighbor group.	
Configuration Examples	The following example transmits community attributes to the specified BGP neighbor. FS(config-router)# neighbor 10.1.1.1 send-community both	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	ip community-list	Creates the community list.
Platform Description	None	

5.113 neighbor shutdown

	Use this command to disconnect the BGP connection established with the specified BGP peer. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} shutdown no neighbor {peer-address peer-group-name} shutdown default neighbor { peer-address peer-group-name } shutdown	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to disconnect valid connection established with the specified peer (group), and delete all associated routing information. However, this command still keeps the configuration information of that specified peer (group). If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example disconnects the BGP connection established with the specified BGP peer. FS(config)# router bgp 60	

	FS(config-router)# neighbor 10.0.0.1 shutdown	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	show ip bgp summary	Displays the BGP connection status.
Platform Description	None	

5.114 neighbor soft-reconfiguration inbound

	Use this command to store the routing information sent from the BGP peer. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} soft-reconfiguration inbound no neighbor {peer-address peer-group-name} soft-reconfiguration inbound default neighbor { peer-address peer-group-name } soft-reconfiguration inbound	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4 Unicast VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP VPNv4/VPNv6 address family configuration mode, BGP scope configuration mode	
Usage Guide	This command restarts the BGP session, and keeps the unchanged routing information sent from the BGP peer (group). Executing this command will consume more memories. If both parties support the route refresh function, this command becomes unnecessary. You may run the show ip bgp neighbors command to judge whether the peer can support the route refresh function. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example stores the routing information sent from the BGP peer. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 soft-reconfiguration inbound</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	show ip bgp neighbors	Displays the information of the BGP peer.
	clear ip bgp	Resets the BGP peer session.
Platform Description	None	

5.115 neighbor timers

	In specifying BGP peer to establish the BGP connection, use this command to set the keepalive and holdtime time values used for establishing the BGP connection. Use the no or default form of this command to restore the default setting. <pre>neighbor {peer-address peer-group-name} timers keepalive holdtime [minimum-holdtime] connect connect-retry }</pre> <pre>no neighbor [peer-address peer-group-name] timers [connect]</pre> <pre>default neighbor { peer-address peer-group-name } timers [connect]</pre>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>keepalive</i>	Time interval to send the KEEPALIVE message to the BGP peer. Range: 0-65535 seconds
	<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds
	<i>minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.
	<i>connect-retry</i>	The value of the connect-retry timer is 15s.
Defaults	<pre>keepalive: 60 seconds</pre> <pre>holdtime: 180 seconds</pre> <pre>minimum-holdtime: 0 seconds</pre> <pre>connect-retry: 15 seconds</pre>	
Command Mode	BGP configuration mode, BGP IPv4 VRF address family configuration mode, BGP IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	A proper keepalive value must not exceed one-third of the holdtime value. If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example sets the keepalive and holdtime time values used for establishing the BGP connection. <pre>FS(config)# router bgp 65000</pre> <pre>FS(config-router)# neighbor 10.0.0.1 80 240</pre>	
	The following example sets the connect-retry time values used for establishing the BGP connection. <pre>FS(config)# router bgp 65000</pre> <pre>FS(config-router)# neighbor 10.0.0.1 timers connect 100</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.

	timers bgp	Sets the keepalive and holdtime values globally.
Platform		
Description	None	

5.116 neighbor unsuppress-map

	Use this command to selectively advertise routing information suppressed by aggregate-address command. Use the no or default form of this command to restore the default setting. neighbor {peer-address peer-group-name} unsuppress-map map-tag no neighbor {peer-address peer-group-name} unsuppress-map map-tag default neighbor { peer-address peer-group-name } unsuppress-map map-tag	
Parameter	Parameter	Description
	<i>peer-address</i>	IP address of the peer
Description	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>map-tag</i>	Name of the route-map of up to 32 characters
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP L2VPN EVPN address family configuration mode BGP VPNv4/VPNv6 address family configuration mode, BGP scope configuration mode	
Usage Guide	This command advertises the specified suppressed routes. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example selectively advertises routing information suppressed by aggregate-address command. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 unsuppress-map unspress-route</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
	aggregate-address	Configures the aggregate address.
	route-map	Configures the route-map
Platform		
Description	None	

5.117 neighbor update-delay

	Use this command to configure the time of BGP delayed advertisement for first routes. Use the no or restore form of the command to restore the default setting. neighbor { peer-address peer-group-name } update-delay time no neighbor { peer-address peer-group-name } update-delay default neighbor { peer-address peer-group-name } update-delay

Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>time</i>	Time of BGP delayed advertisement for first routes.
Defaults	The function is disabled by default.	
Command Mode	BGP configuration mode/ BGP IPv4 VRF address family configuration mode/ BGP IPv6 VRF address family configuration mode/ BGP scope configuration mode	
Usage Guide	After BGP starts, BGP peers negotiate to establish the neighborhood before sending route information (update packets). In addition, after update-delay is configured on the local end, a specific neighbor sends route information to the local end, the local end will send out the route information after the delay time. If the BGP peer group is specified, all members of the peer group adopt the settings of this command.	
Configuration Examples	The following example sets the delayed time to 60s. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 update-delay 60</pre>	
Platform Description	N/A	

5.118 neighbor update-source

	Use this command to configure the interface for BGP connection of the IBGP peer.. neighbor { peer-address peer-group-name } update-source {interface-type interface-number address } Use the no form of the command to remove the source address configuration for the BGP peer. no neighbor {peer-address peer-group-name} update-source Use the default form of the command to restore the default settings. default neighbor { peer-address peer-group-name } update-source	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer, IPv4 or IPv6 address
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>interface-type interface-number</i>	Interface name
	<i>address</i>	The interface address which is used for BGP connection. The address type (IPv4 or IPv6) must be same as that of the peer address.
Defaults	The local interface is used as the egress interface by default.	
Command Mode	BGP configuration mode/ IPv4 VRF address family configuration mode/ IPv6 VRF address family configuration mode/ Scope configuration mode	
Usage Guide	You can use this command to enable the loopback interface to establish a BGP connection with the peer. The interface address specified for BGP connection must be valid in local, otherwise the BGP connection may be faulty. All members in a BGP peer group inherit the settings of this command. Particularly, if the interface address is used,	

	only the member whose address type is same as the interface address's can inherit the settings of this command. If the IPv6 address of the loopback interface is used for neighbor connection, both peers need to be configured with the loopback interface. The BGP connection can be established only when the address of the egress interface on the peer is same as that of the neighbor in local. A loopback interface address can be configured on different interfaces. You need to specify only the interface name, The peer configured with the IPv6 address of loopback interface support only one-hop BGP neighbor connection.	
Configuration Examples	The following example establishes the BGP connection. <pre>FS(config)# router bgp 65000 FS(config-router)# neighbor 10.0.0.1 update-source loopback 1</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.119 neighbor version

	Use this command to display the number of the BGP protocol version used by the specific BGP neighbor. Use the no or default form of this command to restore the default setting. <pre>neighbor { peer-address peer-group-name } version 4 no neighbor { peer-address peer-group-name } version default neighbor { peer-address peer-group-name } version</pre>	
Parameter Description	Parameter	Description
	<i>peer-address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>4</i>	Version number
Defaults	The default version number is 4.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode	
Usage Guide	When the command is used, BGP will lose the version negotiation function.	
Configuration Examples	The following example displays the number of the BGP protocol version used by the specific BGP neighbor. <pre>FS(config-router)# neighbor 10.1.1.1 version 4</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.120 neighbor weight

	Use this command to set the weight for the specific neighbor. Use the no or default form of this command to restore the default setting. neighbor { peer-address peer-group-name } weight number no neighbor { peer-address peer-group-name } weight default neighbor { peer-address peer-group-name } weight	
Parameter	Parameter	Description
	<i>peer-address</i>	IP address of the peer
	<i>peer-group-name</i>	Name of the peer group of up to 32 characters
	<i>number</i>	Weight, in the range from 0 to 65535.
Defaults	No weight is configured for the specific neighbor by default. In this case, the learned route weight is 0 and the locally generated route's weight is 32768 initially.	
Command Mode	BGP configuration mode, BGP IPv4 Unicast/VRF address family configuration mode, BGP IPv6 Unicast/VRF address family configuration mode, BGP scope configuration mode and BGP L2VPN EVPN family address configuration mode	
Usage Guide	When the command is used, routes learnt from the neighbor use this value as the initial weight value. The higher the weight, the higher the priority is. Executing the set weight command in the route map of the neighbor will overwrite this value.	
Configuration Examples	The following example sets the weight for the specific neighbor. <pre>FS(config-router)# neighbor 10.1.1.1 weight 73</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	neighbor remote-as	Configures the BGP peer.
Platform Description	None	

5.121 network

	Use this command to configure the network information to be advertised by the local BGP speaker. Use the no or default form of this command to restore the default setting. network network-number [mask mask] [route-map map-tag] [backdoor] no network network-number [mask mask] [route-map map-tag] [backdoor] default network network-number [mask mask] [route-map map-tag] [backdoor]	
Parameter	Parameter	Description
	network-number	Network number
	mask	Subnet mask
	map-tag	Name of the route-map of up to 32 characters
	backdoor	The route is a backdoor route.

Defaults	No network information is specified by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command allows injecting the IGP route into the BGP routing table. The network information advertised can be direct route, static route and dynamic route. The "route-map" can be used to modify the network information.	
Configuration Examples	The following example configures the network information to be advertised by the local BGP speaker. <pre>FS(config)# router bgp 65000 FS(config-router)# network 10.0.0.1 mask 255.255.0.0</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	redistribute	Configures the route redistribution.
	Network synchronization	Enables network synchronization.
Platform Description	None	

5.122 network synchronization

	Use this command to advertise the network information after the local BGP speaker is synchronized with the local device. Use the no or default form of this command to directly advertise the network information. network synchronization no network synchronization default network synchronization	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	This command is used to modify the status of the network during the process of advertisement. It is not recommended to turn off this switch lest route black hole is caused.	
Configuration Examples	The following example advertises the network information after the local BGP speaker is synchronized with the local device. <pre>FS(config)# router bgp 65000 FS(config-router)# network synchronization</pre>	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
	redistribute	Configures the route redistribution.
	network(BGP)	Configures the route to be distributed.
Platform Description	None	

5.123 overflow memory-lack

	Use this command to allow BGP to enter the OVERFLOW state when the memory is insufficient. Use the no or default form of this command to disable this function. overflow memory-lack no overflow memory-lack default overflow memory-lack	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	Allow the BGP to enter the OVERFLOW state when the memory is insufficient.	
Command		
Mode	BGP configuration mode or BGP Scope Global configuration mode	
Usage Guide	In the BGP OVERFLOW state, the newly-learned routes are discarded, which prevents the memory from increasing. When this function is enabled, if the BGP address family is in the OVERFLOW state, the newly-learned routes will be discarded, which may result in network loop. To prevent this, BGP generates a default route directing to the NULL interface, and the default route will always exist in the OVERFLOW state. Use the clear bgp {addressfamily all} * command to reset the BGP and clear the OVERFLOW state in the BGP address family. Use the no option to disallow the BGP to enter the OVERFLOW state when the memory is insufficient, which may lead to the continuous exhaustion of the memory resources. When the memory has been exhausted to a certain degree, BGP will break down all neighbors and delete all learned routes.	
Configuration Examples	The following example sets BGP not to enter the OVERFLOW configuration status when the memory is insufficient. <pre>FS(config)# router bgp 65000 FS(config-router)# no overflow memory-lack</pre>	
Related Commands	Command	Description
	clear bgp { addressfamily all } *	Resets the BGP address family.
	show bgp { addressfamily all } summary	Displays the summary of the BGP address family.
Platform		
Description	None	

5.124 rd

	Use this command to configure a RD value for the EVI instance. Use the no or restore form of this command to restore the default settings. rd { auto rd_value } no rd { auto rd_value } default rd	
Parameter	Parameter	Description
Description	auto	Generates the RD value automatically.

	<i>rd_value</i>	Indicates value of the RD. There are 3 forms of rd_value: 1. <code>rd_value = as_num:nn</code> The as_num indicates the public AS number (2 bytes) and nn is customized. The range is from 0 to 4,294,967,295. 2. <code>rd_value = ip_addr:nn</code> The ip_add refers to the global IP address and nn is customized. The range is from 0 to 65,535. 3. <code>rd_value = as4_num:nn</code> The as4_num indicates the public AS number (2 bytes) and nn is customized. The range is from 0 to 65,535. The 4-byte AS notation range is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode.
Defaults	The RD value is not configured by default.	
Command Mode	evpn-vni configuration mode	
Usage Guide	If an EVI is configured with a RD value, the RD value cannot be revised. If you want to revise it, you can only delete the EVI first and then configure a new RD value for it. One EVI can be configured with one RD value only.  The RD format in 4-byte AS is AS4:NN. The AS4 supports demical and dot mode. The range of AS4 is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode. The range of NN is from 1 to 65,535.  For AS number in the range of 1 to 65,535, it will be saved in the format of 2-byte AS, because under this condition, the demical and dot mode AS are the same. 	
Configuration Examples	The following example sets RD for EVI 100. The value is 100 : 1. <pre>FS(config)# evpn FS(config-evpn)# vni 100 FS(config-evpn-vni)# rd 100:1</pre> The following example sets RD for EVI 200. The value is auto. <pre>FS(config)# evpn FS(config-evpn)# vni 200 FS(config-evpn-vni)# rd auto</pre>	
Platform Description	N/A	

5.125 redistribute

	Use this to redistribute routes between the other routing protocol and the BGP. Use the no or default form of this command to restore the default setting. <code>redistribute protocol-type [route-map map-tag] [metric metric-value]</code> <code>no redistribute protocol-type [route-map map-tag] [metric]</code> <code>default redistribute protocol-type [route-map map-tag] [metric]</code>

Parameter Description	Parameter	Description
	<i>protocol-type</i>	The source protocol types for redistributing routes, including connected, static, RIP
	route-map <i>map-tag</i>	Specifies the route map. No route map is associated with by default.
	metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols.  When you configure the no form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured.  The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.	
Configuration Examples	The following example redistributes routes between the other routing protocol and the BGP. <pre>FS(config-router)# redistribute static route-map static-rmap</pre>	
Related Commands	Command	Description
	show ip protocol	Displays the protocol configuration.
Platform Description	None	

5.126 redistribute ospf

	Use this command to redistribute routes between OSPF and BGP. Use the no or default form of this command to restore the default setting. <pre>redistribute ospf process-id [route-map map-tag] [metric metric-value] [match internal external [1 2] nssa-external [1 2]]</pre> <pre>no redistribute ospf process-id [route-map map-tag] [metric metric-value] [match internal external [1 2] nssa-external [1 2]]</pre> <pre>default redistribute ospf process-id [route-map map-tag] [metric] [match { internal external [1 2] nssa-external [1 2] }</pre>	
Parameter Description	Parameter	Description
	process-id	OSPF process ID to be redistributed
	route-map <i>map-tag</i>	Specifies the route map. No route map is associated by default.
	metric <i>metric-value</i>	Sets the default metric of the routes to be redistributed, null by default.
	match	Matches the sub type of OSPF routes.
	internal	Matches the internal OSPF routes, the default configuration.

	external [1 2]	Matches the external OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
	nssa- external [1 2]	Matches the NSSA-external type of OSPF routes. You can specify the concrete type (v1 or v2) or v1 and v2 without indication.
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol.  When you configure the no form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured.  The filtering rule of OSPF routing: filtering the OSPF routing type according to the configured match option before filtering the route-map rule. The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are not available, the redistributed one is used.	
Configuration Examples	The following example redistributes routes between OSPF and BGP. <pre>FS(config-router)# redistribute ospf 2 route-map static-rmap</pre>	
Related Commands	Command	Description
	show ip protocol	Displays the protocol configuration.
Platform Description	None	

5.127 redistribute isis

	Use this command to redistribute routes between ISIS and BGP. Use the no or default form of this command to restore the default settings. redistribute isis [isis-tag] [route-map map-tag] [metric metric-value] [level-1 level-1-2 level-2] no redistribute isis [isis-tag] [route-map map-tag] [metric] [level-1 level-1-2 level-2] default redistribute isis [isis-tag] [route-map map-tag] [metric] [level-1 level-1-2 level-2]	
Parameter Description	Parameter	Description
	isis-tag	(Optional)ISIS process ID to be redistributed
	route-map map-tag	Specifies the route map. No route map is associated by default.
	metric metric-value	Sets the default metric of the routes to be redistributed, null by default.
	level-1	Redistributes level-1 ISIS routes.
	level-1-2	Redistributes level-1 and level-2 ISIS routes.
	level-2	Redistributes level-2 ISIS routes.
Defaults	This function is disabled by default.	

Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. The switch may run multiple routing protocols at the same time, so it should redistribute a protocol's information to another protocol. This is applicable to all IP routing protocols. When you configure the no form of this command with parameters, the corresponding parameter configuration will be removed. The no form removes redistribution without any parameters configured. The filtering rule of ISIS routing is: filtering the ISIS routing type according to the configured level option before filtering the route-map rule. The route metric generated by the route-map command takes precedence over the one generated by the metric option of this command. If both are unavailable, the redistributed one is used.	
Configuration Examples	The following example redistributes routes between ISIS and BGP. <pre>FS(config-router)# redistribute isis route-map static-rmap</pre>	
Related Commands	Command	Description
	show ip protocol	Displays the protocol configuration.
Platform Description	None	

5.128 route-target

	Use this command to configure a RT (Route Target) for EVI. Use the no or restore form of this command to restore the default settings. <pre>route-target { import export both } { auto rt_value } no route-target { import export both } { auto rt_value } default route-target { import export both } { auto rt_value }</pre>	
Parameter Description	Parameter	Description
	auto	Generates the RD value automatically.
	import	Sets the import RT value.
	export	Sets the export RT value.
	both	Sets the import and export RT value.
	rt_value	Indicates value of the RT. There are 3 forms of rt_value: - rt_value = as_num:nn The as_num indicates the public AS number (2 bytes) and nn is customized. The range is from 0 to 4,294,967,295. - rt_value = ip_addr:nn The ip_add refers to the global IP address and nn is customized. The range is from 0 to 65,535. - rt_value = as4_num:nn The as4_num indicates the public AS number (2 bytes) and nn is customized. The range is from 0 to 65,535. The 4-byte AS notation range is from 1 to 4,294,967,295, represented as from 1 to 65535.65535 in dot mode.
Defaults	The RT value is not configured by default.	

Command	
Mode	evpn-vni configuration mode
Usage Guide	One EVI can be configured with multiple import and export RT values.  The format of auto RT is AS2:nn. The AS2 is the AS number of 2B. If an AS number of 4B is configured, it will be split into two 2B AS number and then be put in the RT. The nn indicates value of vni-id and has a space of 4B.  If the AS number of BGP changes, the auto RT will be changed, too.  If the manually configured RT is coherent with the auto RT, both will be displayed. After the auto command is configured and the automatically generated RT value is 100 : 1, then if you delete value 100 : 1, only the value not the auto command will be deleted.
Configuration Examples	The following example sets RT for EVI 100. The values are import RT 100:1, 100:4, export RT 100:2, 100:4, and both auto. <pre>FS(config)# evpn FS(config-evpn)# vni 100 FS(config-evpn-vni)# route-target import 100:1 FS(config-evpn-vni)# route-target export 100:2 FS(config-evpn-vni)# route-target both 100:4 FS(config-evpn-vni)# route-target both auto</pre>
Platform Description	N/A

5.129 router bgp

	Use this command to enable the BGP protocol, configure the local autonomous system number and enter BGP protocol configuration mode. Use the no or default form of this command to restore the default setting. router bgp as-number no router bgp as-number default router bgp as-number	
Parameter Description	Parameter	Description
	<i>as-number</i>	AS number in the range from 1 to 65535 In the 10.4(3) or later versions, the 4-byte AS notation is supported, namely, the new AS notation range is from 1 to 4294967295, represented as from 1 to 65535.65535 in dot mode.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to start the BGP protocol. RFC4839 defines a new reserved AS notation 23456, which cannot be used. The original private AS notation in the range from 64512 to 65534 is still effective, 65535 is reserved for special purposes. RFC 5398 also defines two groups of new reserved AS notation for documents, whose ranges are from 64496 to	

	64511 and from 65536 to 65551.	
Configuration Examples	The following example enables the BGP protocol. FS(config)# router bgp 65000	
Related Commands	Command	Description
	ip routing	Enables IP routing.
	bgp router-id	Sets the ID of the device running the BGP protocol
	network	Sets the network information to be advertised by the local BGP speaker.
Platform Description	None	

5.130 synchronization

	Use this command to enable the synchronization mechanism of BGP and IGP routing information. Use the no or default form of this command to restore the default settings. synchronization no synchronization default synchronization	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	The synchronization between BGP and IGP aims to prevent the possible route black hole. In any of the two cases below, you may cancel the synchronization mechanism to ensure fast convergence of routing information. - There is no route information which passes through this AS (In general, this AS is an end AS). - All devices within this AS operate BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).	
Configuration Examples	The following example enables the synchronization mechanism of BGP and IGP routing information. FS(config)# router bgp 65000 FS(config-router)# synchronization	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol.
Platform Description	None	

5.131 table-map

	Use this command to control the route information distributed to the kernel table. Use the no or default form of this command to restore the default setting.

	table-map route-map-name no table-map default table-map	
Parameter	Parameter	Description
Description	<i>route-map-name</i>	Name of the route-map
Defaults	No table-map is configured by default,	
Command Mode	BGP configuration mode, BGP IPv4/IPv6 Unicast address family configuration mode, BGP IPv4/IPv6 VRF address family configuration mode or BGP Scope configuration mode.	
Usage Guide	BGP uses the table-map to control the information distributed to the kernel routing table. The table-map is used to modify attributes of that route information, and it only takes effect on the IPv4 address-family.	
Configuration Examples	The following example controls the route information distributed to the kernel table. <pre>FS(config)# router bgp 65000 FS(config-router)# table-map bgp_tm</pre>	
Related Commands	Command	Description
	route-map	Configures the route-map
Platform Description	None	

5.132 timers bgp

	Use this command to adjust the BGP network timer. Use the no or default form of this command to restore the default value. timers bgp keepalive holdtime [minimum-holdtime] no timers bgp default timers bgp	
Parameter Description	Parameter	Description
	<i>keepalive</i>	Time interval to send the keepalive message to the BGP peer Range: 0-65535 seconds.
	<i>holdtime</i>	Time interval to consider the BGP peer alive Range: 0-65535 seconds.
	<i>Minimum-holdtime</i>	Allows a minimum holdtime value of neighbor advertisement. It is unrestricted when the value is 0. The range is 0 to 65535 seconds.
Defaults	<i>keepalive</i> : 60 seconds <i>holdtime</i> : 180 seconds <i>minum-holdtime</i> : 0 seconds	
Command Mode	BGP configuration mode / BGP scope global configuration mode	
Usage Guide	A proper keepalive value must not exceed one-third of the holdtime value.	

	If the time is configured for an individual peer or a peer group, that peer or peer-group will use its time to replace the global time configuration and connect the peer. If the BGP peer group is specified, all members of the peer group adopt the settings of this command. If this command is set for a member of the peer, the setting will overwrite the setting for the group.	
Configuration Examples	The following example adjusts the BGP network timer. <pre>FS(config)# router bgp 65000 FS(config-router)# timers bgp 80 240</pre>	
Related Commands	Command	Description
	neighbor timers	Sets the keepalive and holdtime values on the basis of neighbors.
Platform Description	None	

5.133 show bgp all

Use this command to display all the address-families information of BGP route. The use of this command is consistent with other BGP's show commands.

Display the parameters of the route information.

`show bgp all [ community [ community-number [ exact-match ] ] | filter-list path-list-number | community-list community-name [ exact-match ] | extcommunity-list extcommunity-name | regexp regexp | quote-regexp regexp | inconsistent-as ]`

Display the route dampening parameter.

`show bgp all dampening { flap-statistics | dampened-paths | parameters }`

Display the related information of the neighbors.

`show bgp all neighbors [ peer-address [ received-routes | routes | advertised-routes | policy [ detail ] ] ]`

`show bgp all summary`

Display the update-group information.

`show bgp [ instance as-num ] all update-group [ neighbor-address | update-group-index ] [ summary ]`

Parameter Description	Parameter	Description
	community <i>community-number</i>	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
	community-list <i>community-name</i>	Displays the BGP routing information matching the specified community-list.
	exact-match	Routing information exactly matching the community value or community-list.
	dampening dampened-paths	Displays the restrained routing information.
	dampening flap-statistics	Displays the routing dampening statistics.
	dampening parameters	Displays the routing dampening parameters.
	extcommunity-list <i>extcommunity-name</i>	Displays the routing information including the specified extcommunity value.
	filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
	inconsistent-as	Displays the routing information of the inconsistent source AS.
	neighbors [<i>peer-address</i>]	Displays all the BGP neighbors' information.
	neighbors <i>peer-address</i> received-routes	Displays all routing information received from the specified peer (including the accepted and refused route).
	neighbors <i>peer-address</i> routes	Displays all the accepted routing information received from the peer.
	neighbors <i>peer-address</i> advertised-routes	Displays all the routing information sent to the

		specified peer.												
	neighbors <i>peer-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)												
	neighbors <i>peer-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)												
	quote-regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.												
	regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp.												
	Summary	Displays BGP neighbor information.												
	update-group [<i>neighbor-address</i> <i>update-group-index</i>]	Display update-group information. When <i>neighbor-address</i> is specified, display the update-group information of the specified neighbor. When <i>update-group-index</i> is specified, display the specified update-group information.												
Command Mode	Privileged EXEC mode													
Usage Guide	N/A													
Configuration Examples	The following example shows all neighbors' information.													
	<pre>FS(config)# show bgp all</pre>													
	For address family: IPv4 Unicast													
	BGP table version is 1, local router ID is 1.2.3.4													
	Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,													
	S Stale													
	Origin codes: i - IGP, e - EGP, ? - incomplete													
	<table><thead><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr></thead><tbody><tr><td>*> 1.0.0.0</td><td>0.0.0.0</td><td>0</td><td></td><td>32768</td><td>?</td></tr></tbody></table>		Network	Next Hop	Metric	LocPrf	Weight	Path	*> 1.0.0.0	0.0.0.0	0		32768	?
	Network	Next Hop	Metric	LocPrf	Weight	Path								
	*> 1.0.0.0	0.0.0.0	0		32768	?								
Total number of prefixes 1														
For address family: IPv6 Unicast														
BGP table version is 1, local router ID is 1.2.3.4														
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,														

	S Stale				
	Origin codes: i - IGP, e - EGP, ? - incomplete				
	Network	Next Hop	Metric	LocPrf	Weight Path
	*> 5750:1::/120	::	0		32768 ?
	Total number of prefixes 1				
Related	Command		Description		
Commands	show bgp ipv4 unicast		Displays the IPv4 unicast route information of BGP		
Platform					
Description	None				

5.134 show bgp ipv4 unicast

	Use this command to display the IPv4 unicast route information of BGP. <pre>show bgp ipv4 unicast [vrf vrf-name] [network [network-mask [longer-prefixes]]] show bgp ipv4 unicast [vrf vrf-name] community community-number [exact-match] show bgp ipv4 unicast [vrf vrf-name] community-list community-name [exact-match] show bgp ipv4 unicast [vrf vrf-name] extcommunity-list extcommunity-name show bgp ipv4 unicast [vrf vrf-name] dampening dampened-paths show bgp ipv4 unicast [vrf vrf-name] dampening flap-statistics show bgp ipv4 unicast [vrf vrf-name] filter-list path-list-number show bgp ipv4 unicast [vrf vrf-name] inconsistent-as show bgp ipv4 unicast [vrf vrf-name] prefix-list ip-prefix-list-name show bgp ipv4 unicast [vrf vrf-name] quote-regexp regexp show bgp ipv4 unicast [vrf vrf-name] regexp regexp show bgp ipv4 unicast [vrf vrf-name] route-map map-tag show bgp ipv4 unicast [vrf vrf-name] neighbors [neighbor-address [received-routes routes advertised-routes policy [detail]]] show bgp ipv4 unicast [vrf vrf-name] cidr-only</pre>	
	Parameter	Description
Parameter Description	vrf-name	VRF name
	network	Displays the specific routing information in the routing table
	network-mask	Displays the routing information included in the specified network.
	longer-prefixes	Displays the route map information.
	community community-number	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
	community-list community-name	Displays the BGP routing information matching the specified community-list.

	exact-match	Routing information exactly matching the community value or community-list.
	extcommunity-list extcommunity-name	Displays the routing information including the specified extcommunity value.
	dampening dampened-paths	Displays the restrained routing information.
	dampening flap-statistics	Displays the routing dampening statistics.
	filter-list path-list-number	Displays the routing information matching the filter-list.
	inconsistent-as	Displays the routing information of the inconsistent source AS.
	prefix-list ip-prefix-list-name	Displays the routing information matching the specified prefix-list.
	quote-regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
	regexp regexp	Displays the BGP routing information with the AS path attribute matching the specified regexp.
	route-map map-tag	Displays the routing information matching the specified route-map filtering condition.
	neighbors [neighbor-address]	Displays the BGP IPv4 unicast neighbor information.
	neighbors neighbor-address received-routes	Displays all routing information received from the specified peer (including the accepted and refused route).
	neighbors neighbor-address routes	Displays all the routing information received from the peer and accepted.
	neighbors neighbor-address advertised-routes	Displays all the routing information sent to the specified peer.
	neighbors neighbor-address policy	Displays the related routing policy information of BGP neighbors. (General)
	neighbors neighbor-address policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
	cidr-only	Displays the routing information without the category.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to view the IPv4 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information.	
Configuration Examples	The following example displays the IPv4 unicast route information of BGP. <pre> FS# show bgp ipv4 unicast BGP table version is 2, local router ID is 192.168.183.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Path *>i44.0.0.0 192.168.195.183 0 100 i *>i64.12.0.0/16 192.168.195.183 0 100 i *>i172.16.0.0/24 192.168.195.183 0 100 i *>i202.201.0.0 192.168.195.183 0 100 i *>i202.201.1.0 192.168.195.183 0 100 i </pre>	

```

*>i202.201.2.0 192.168.195.183 0 100 i
*>i202.201.3.0 192.168.195.183 0 100 i
*>i202.201.18.0 192.168.195.183 0 100 i
Total number of prefixes 8
FS# show bgp ipv4 unicast community 11:2222
111:12345
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network    Next Hop    Metric  LocPrf Path
*>i202.201.0.0 192.168.195.183 0 100 i
*>i202.201.1.0 192.168.195.183 0 100 i
*>i202.201.2.0 192.168.195.183 0 100 i
*>i202.201.3.0 192.168.195.183 0 100 i
Total number of prefixes 4
FS(config)# ip as-path access-list 5 permit .*
FS# show bgp ipv4 unicast filter-list 5
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network    Next Hop    Metric  LocPrf Path
*>192.168.88.0 0.0.0.0 32768 ?
Total number of prefixes 1
FS# show ip bgp cidr-only
BGP table version is 2, local router ID is 192.168.183.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network    Next Hop    Metric  LocPrf Path
*>i64.12.0.0/16 192.168.195.183 0 100 i
*>i172.16.0.0/24 192.168.195.183 0 100 i
Total number of prefixes 2
FS# show bgp ipv4 unicast labels
Network    Next Hop    In Label/Out Label
1.1.1.1/32 192.167.1.1 17/18
1.1.1.2/32 192.167.1.1 nolabel/19

```

Field	Description
Network	Route prefix
Nexthop	Nexthop IP address of the route
In label	Label assigned by this router (if any).

	Out label	Label learnt from the nexthop router (if any).	
Related Commands	Command	Description	
	show ip bgp	Displays the IPv4 unicast route information of BGP.	
Platform			
Description	None		

5.135 show bgp ipv4 unicast dampening parameters

	Use this command to display the IPv4 unicast route dampening parameters configured for the BGP. show bgp ipv4 unicast [vrf vrf-name] dampening parameters		
Parameter	Parameter	Description	
Description	<i>vrf-name</i>	VRF name	
Defaults	N/A		
Command Mode	Privileged EXEC mode		
Usage Guide	This command is used to display the IPv4 unicast route dampening parameters configured for BGP.		
Configuration Examples	The following example displays the IPv4 unicast route dampening parameters configured for the BGP. <pre>FS(config-router)# bgp dampening 25 10000 10000 200 FS# show bgp ipv4 unicast dampening parameters dampening 25 10000 10000 200 Dampening Control Block(s): Reachability Half-Life time : 25 min Reuse penalty : 10000 Suppress penalty : 10000 Max suppress time : 200 min Max penalty (ceil) : 29800000 Min penalty (floor) : 5000</pre>		
Related Commands	N/A		
Platform			
Description	None		

5.136 show bgp ipv4 unicast neighbors

	Use this command to display the related information of BGP IPv4 unicast neighbor. show bgp ipv4 unicast [vrf vrf-name] neighbors neighbor-address	
Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name
	<i>neighbor-address</i>	Neighbor IPv4 address
	neighbors neighbor-address policy	Displays the related routing policy information of BGP

		neighbors. (General)
	neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to view the information of the connection with BGP IPv4 unicast neighbor.	
Configuration Examples	The following example displays the related information of BGP IPv4 unicast neighbor. <pre> FS# show bgp ipv4 unicast neighbors BGP neighbor is 192.168.195.183, remote AS 23, local AS 23, internal link BGP version 4, remote router ID 44.0.0.1 BGP state = Established, up for 00:06:37 Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds Neighbor capabilities: Route refresh: advertised and received (old and new) Address family IPv4 Unicast: advertised and received Graceful restart: advertised and received Remote Restart timer is 120 seconds Received 14 messages, 0 notifications, 0 in queue open message:1 update message:4 keepalive message:9 refresh message:0 dynamic cap:0 notifications:0 Sent 12 messages, 0 notifications, 0 in queue open message:1 update message:3 keepalive message:8 refresh message:0 dynamic cap:0 notifications:0 Route refresh request: received 0, sent 0 Minimum time between advertisement runs is 0 seconds For address family: IPv4 Unicast BGP table version 2, neighbor version 1 Index 2, Offset 0, Mask 0x4 Inbound soft reconfiguration allowed 8 accepted prefixes 0 announced prefixes Connections established 2; dropped 1 Local host: 192.168.195.239, Local port: 1074 Foreign host: 192.168.195.183, Foreign port: 179 Nexthop: 192.168.195.239 Nexthop global: :: Nexthop local: :: BGP connection: non shared network Last Reset: 00:06:43, due to BGP Notification sent Notification Error Message: (Cease/Unspecified Error Subcode) Using BFD to detect fast fallover </pre>	
Related	N/A	

Commands	
Platform	
Description	None

5.137 show bgp ipv4 unicast paths

	Use this command to display the path information of the IPv4 unicast in the route database. show bgp ipv4 unicast [vrf vrf-name] paths	
Parameter	Parameter	Description
Description	vrf-name	VRF name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to view the path information in the route database.	
Configuration Examples	The following example displays the path information of the IPv4 unicast in the route database. <pre>FS# show bgp ipv4 unicast paths Address Refcnt Path [0x1d7806a0:0] (67) [0x1d7389a0:13] (20) 10</pre>	
Related Commands	N/A	
Platform Description	None	

5.138 show bgp ipv4 unicast summary

	Use this command to display the related information of BGP IPv4 unicast. show bgp ipv4 unicast [vrf vrf-name] summary	
Parameter	Parameter	Description
Description	vrf-name	VRF name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the related information of BGP IPv4 unicast.	
Configuration Examples	The following example displays the related information of BGP IPv4 unicast. <pre>FS # show bgp ipv4 unicast summary</pre>	

	BGP router identifier 192.168.183.1, local AS number 23 BGP table version is 2 2 BGP AS-PATH entries 1 BGP community entries Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 192.168.195.79 4 24 0 0 0 0 0 never Active 192.168.195.183 4 23 17 15 1 0 0 00:09:04 8 Total number of neighbors 2	
Related	Command	Description
Commands	router bgp	Enables the BGP protocol
Platform		
Description	None	

5.139 show bgp ipv4 unicast update-group

	Use this command to display information about an update-group in the BGP IPv4 unicast address family. show bgp ipv4 unicast [vrf vrf-name] update-group [neighbor-address update-group-index] [summary]	
Parameter	Parameter	Description
Description	<i>vrf-name</i>	Specifies a VRF instance name.
	<i>neighbor-address</i>	Specifies a neighbor that belongs to an update-group whose information needs to be displayed.
	<i>update-group-index</i>	Specifies an update-group whose information needs to be displayed.
	summary	Displays neighbor-related information.
Command	Privileged EXEC mode	
Mode		
Default Level	14	
Usage Guide	This command is used to display information about an update-group in the BGP IPv4 unicast address family.	
Configuration	The following example displays information about an update-group in the BGP IPv4 unicast address family.	
Example	<pre> FS#show bgp ipv4 update-group BGP version 4 update-group 1(ref 2), internal, Address Family: IPv4 Unicast Update message formatted 2, replicated 2 Minimum route advertisement interval is 0 seconds Minimum AS origination interval is 1 seconds Format state: Current working Refresh blocked Has 1 members: </pre>	

192.168.195.183

The following example displays the neighbor summary of update-group 1 in the BGP IPv4 unicast address family.

```
FS # show bgp ipv4 unicast update-group 1 summary
```

```
BGP router identifier 192.168.183.1, local AS number 23
```

```
BGP table version is 2
```

```
2 BGP AS-PATH entries
```

```
1 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.195.79	4	24	0	0	0	0	0	never	Active
192.168.195.183	4	23	17	15	1	0	0	00:09:04	8

```
Total number of neighbors 2
```

Field description:

Field	Description
BGP router identifier	BGP router ID
local AS number	Local AS number of BGP
BGP table version	Version of the BGP routing table
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version
AS	Peer AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	Status of the neighbor state machine or number of received routing entries

5.140 show bgp ipv6 unicast

Use this command to display the IPv6 unicast routing information of BGP.

```
show bgp ipv6 unicast [ vrf vrf-name ] [ ipv6-prefix [ longer-prefixes ] ]
```

```
show bgp ipv6 unicast [ vrf vrf-name ]community community-number [exact-match]
```

```
show bgp ipv6 unicast [ vrf vrf-name ]community-list community-name [exact-match]
```

```
show bgp ipv6 unicast [ vrf vrf-name ] extcommunity-list extcommunity-name
```

```
show bgp ipv6 unicast [ vrf vrf-name ]dampening dampened-paths
```

```
show bgp ipv6 unicast [ vrf vrf-name ]dampening flap-statistics
```

```
show bgp ipv6 unicast [ vrf vrf-name ]filter-list path-list-number
```

```
show bgp ipv6 unicast [ vrf vrf-name ]inconsistent-as
```

```
show bgp ipv6 unicast [ vrf vrf-name ]prefix-list ipv6-prefix-list-name
```

```
show bgp ipv6 unicast [ vrf vrf-name ]quote-regexp regexp
```

```
show bgp ipv6 unicast [ vrf vrf-name ] regexp regexp
```

```
show bgp ipv6 unicast[ vrf vrf-name ] route-map map-tag
```

	show bgp ipv6 unicast [vrf vrf-name] neighbors [neighbor-address [received-routes routes advertised-routes policy [detail]]]	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	<i>IPv6-prefix</i>	Displays the IPv6 routing information included in the specified network. The input format of the routing information prefix is X:X:X:X::X/<0-128>.
	longer-prefixes	Displays the route map information.
	community <i>community-number</i>	Displays the routing information including the specified community value. Community-number can be in the format of AA:NN (autonomous system number / 2-byte number), or the following pre-defined value: internet, no-export, local-as, no-advertise.
	community-list <i>community-name</i>	Displays the BGP routing information matching the specified community-list.
	exact-match	Routing information exactly matches the community value or community-list.
	extcommunity-list <i>extcommunity-name</i>	Displays the routing information including the specified extcommunity value.
	dampening dampened-paths	Displays the restrained routing information.
	dampening flap-statistics	Displays the routing dampening statistics.
	filter-list <i>path-list-number</i>	Displays the routing information matching the filter-list.
	inconsistent-as	Displays the routing information of the inconsistent source AS.
	prefix-list <i>ipv6-prefix-list-name</i>	Displays the routing information matching the specified prefix-list.
	quote-regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp within the double quote marks.
	regexp <i>regexp</i>	Displays the BGP routing information with the AS path attribute matching the specified regexp.
	route-map <i>map-tag</i>	Displays the routing information matching the specified route-map filtering condition.
	neighbors [<i>neighbor-address</i>]	Displays the BGP IPv6 unicast neighbor information.
	neighbors <i>neighbor-address</i> received-routes	Displays all routing information received from the specified peer (including accepted and refused routes).
	neighbors <i>neighbor-address</i> routes	Displays all the routing information received from the peer and accepted.
	neighbors <i>neighbor-address</i> advertised-routes	Displays all the routing information sent to the specified peer.
	neighbors <i>neighbor-address</i> policy	Displays the related routing policy information of BGP neighbors. (General)
	neighbors <i>neighbor-address</i> policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
Defaults	N/A	

Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to view the IPv6 unicast route information of BGP. You can filter the information with the specified parameter to display the matching route information. The function and use of this command is similar to the show bgp ipv4 unicast command, please refer to the command.	
Configuration Examples	N/A	
Related Commands	Command	Description
	show bgp ipv4 unicast	Displays the IPv4 unicast route information of BGP.
Platform Description	None	

5.141 show bgp ipv6 unicast dampening parameters

	Use this command to display the IPv6 unicast route dampening parameters configured for BGP. show bgp ipv6 unicast [vrf vrf-name] dampening parameters	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the IPv6 unicast route dampening parameters configured for the BGP. The function and use of this command are similar to the show bgp ipv4 unicast dampening parameters command. Please refer to the command.	
Configuration Examples	N/A	
Related Commands	Command	Description
	show bgp ipv4 unicast dampening parameters	Displays the IPv4 unicast route dampening parameters configured for BGP.
Platform Description	None	

5.142 show bgp ipv6 unicast neighbors

	Use this command to display the related information of BGP IPv6 unicast neighbor. show bgp ipv6 unicast [vrf vrf-name] neighbors neighbor-address	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
	<i>neighbor-address</i>	Neighbor IPv6 address.

	neighbors neighbor-address policy	Related route policy information of BGP neighbor. (General)
	neighbors neighbor-address policy detail	Related route policy information of BGP neighbor. (Detail)
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to view the information of the connection with BGP IPv6 unicast neighbor. The function and use of this command are similar to the show bgp ipv4 unicast neighbors neighbor-address command. Please refer to the command.	
Configuration Examples	N/A	
Related Commands	Command	Description
	show bgp ipv4 unicast neighbors neighbor-address	Displays the related information of BGP IPv4 unicast neighbor.
Platform Description	None	

5.143 show bgp ipv6 unicast paths

	Use this command to display the path information of the IPv6 unicast in the route database. show bgp ipv6 unicast [vrf vrf-name] paths	
Parameter Description	Parameter	Description
	vrf-name	VRF name
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to view the path information in the route database.	
Configuration Examples	The following example displays the path information of the IPv6 unicast in the route database. <pre>FS# show bgp ipv6 unicast paths Address Refcnt Path [0x1d7806a0:0] (67) [0x1d7389a0:13] (20) 10</pre>	
Related Commands	Command	Description
	show bgp ipv4 unicast paths	Displays the path information of the IPv4 unicast in the route database.
Platform Description	None	

5.144 show bgp ipv6 unicast summary

	Use this command to display the related information of BGP IPv6 unicast. show bgp ipv6 unicast [vrf vrf-name] summary	
Parameter	Parameter	Description
Description	vrf-name	VRF name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the related information of BGP IPv6 unicast. The function and use of this command are similar to the show bgp ipv4 unicast summary command. Please refer to the command.	
Configuration Examples	N/A	
Related Commands	Command	Description
	router bgp	Enables the BGP protocol
	show bgp ipv4 unicast summary	Displays the related information of BGP IPv4 unicast.
Platform Description	None	

5.145 show bgp ipv6 unicast update-group

	Use this command to display information about an update-group in the BGP IPv6 unicast address family. show bgp ipv6 unicast [vrf vrf-name] update-group [neighbor-address update-group-index] [summary]	
Parameter Description	Parameter	Description
	vrf-name	Specifies a VRF instance name.
	neighbor-address	Specifies a neighbor that belongs to an update-group whose information needs to be displayed.
	update-group-index	Specifies an update-group whose information needs to be displayed.
	summary	Displays neighbor-related information.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	This command is used to display information about an update-group in the BGP IPv6 address family.	
Configuration	The following example displays information about an update-group in the BGP IPv6 unicast address family.	

Example

```
FS#show bgp ipv6 update-group

BGP version 4 update-group 1(ref 2), internal, Address Family: IPv6 Unicast

Update message formatted 2, replicated 2

Minimum route advertisement interval is 0 seconds

Minimum AS origination interval is 1 seconds

Format state: Current working

Refresh blocked

Has 1 members:

192:168:195::183
```

The following example displays the neighbor summary of update-group 1 in the BGP IPv6 unicast address family.

```
FS # show bgp ipv6 unicast update-group 1 summary

BGP router identifier 192.168.183.1, local AS number 23

BGP table version is 2

2 BGP AS-PATH entries

1 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192:168:195::79	4	24	0	0	0	0	0	never	Active
192:168:195::183	4	23	17	15	1	0	0	00:09:04	8

```
Total number of neighbors 2
```

Field description:

Field	Description
BGP router identifier	BGP router ID
local AS number	Local AS number of BGP
BGP table version	Version of the BGP routing table
BGP AS-PATH entries	Number of AS path entries
BGP community entries	Number of community attribute entries
Neighbor	Peer address
V	Protocol version
AS	Peer AS number
MsgRcvd	Number of received packets
MsgSent	Number of sent packets
State/PfxRcd	Status of the neighbor state machine or number of received routing entries

Prompt N/A

Platform N/A

Description	

5.146 show bgp l2vpn

Use the following command to display the BGP L2VPN routing information.

```
show bgp l2vpn { evpn } all
```

Use the following command to display the neighbor information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all { ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip } [ detail ]
```

Use the following command to display the second type routing information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all mac-ip mac_addr [ ip_addr [ detail ] | ipv6_addr [ detail ] | detail ]
```

Use the following command to display the fifth type routing information of the BGP L2VPN EVPN address family.

```
show bgp l2vpn evpn all ip-prefix { ip_addr [ detail ] | ipv6_addr [ detail ] | detail }
```

Use the following command to display the neighbor information of the BGP L2VPN address family.

```
show bgp l2vpn { evpn } all neighbor [ peer-address [ policy [ detail ] ] ]
```

Use the following command to display the neighbor summary information of the BGP L2VPN address family.

```
show bgp l2vpn { evpn } all summary
```

Use the following command to display the L2VPN EVPN information on the specified RD.

```
show bgp l2vpn evpn rd vpn_rd [[ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip ] [ detail ]]
```

Use the following command to display the L2VPN EVPN information on the specified EVI.

```
show bgp l2vpn evpn evi vni-id [ [ ethernet-ad | ethernet-segment | inclusive-multicast | ip-prefix | mac-ip ] [ detail ] ]
```

Parameter Description	Parameter	Description
	evpn	Displays EVPN information.
	all	Displays all NLRI information that contains the VPLS instance or the VPWS instance.
	ve_id:offset	Displays the VFI instance information of the specified ve_id:offset
	ethernet-ad [detail]	Displays basic (detailed) information of the first type of BGP L2VPN EVPN routes.
	ethernet-segment [detail]	Displays basic (detailed) information of the fourth type of BGP L2VPN EVPN routes.
	inclusive-multicast [detail]	Displays basic (detailed) information of the third type of BGP L2VPN EVPN routes.
	ip-prefix [detail]	Displays basic (detailed) information of the fifth type of BGP L2VPN EVPN routes.
	ip-prefix [ip_addr [detail] ipv6_addr [detail] detail]	Displays basic (detailed) information of routes with specific IP address or IPv6 address in the fifth type of BGP L2VPN EVPN routes.
	mac-ip [detail]	Displays basic (detailed) information of the second type of BGP L2VPN EVPN routes.
	mac-ip mac_addr [ip_addr [detail] ipv6_addr [detail] detail]	Displays basic (detailed) information of routes with specific MAC addresses or MAC addresses+IP addresses/IPv6 addresses in the

		second type of BGP L2VPN EVPN routes.
	neighbor [peer-address]	Displays the BGP L2VPN neighbor information. You can specify the specific neighbor information by entering the parameter <i>neighbor-address</i> . Otherwise all BGP L2VPN neighbor information is displayed.
	neighbor peer-address policy	Displays the summarized routing policy information on BGP neighbor.
	neighbor peer-address policy detail	Displays the detailed routing policy information BGP neighbor,
	summary	Displays main BGP L2VPN information, including site ID, OFFSET, LABEL BASE and NEXT HOP.
	rd vpn_rd	The specified RD.
	vfi vfi_name	The specified VFI instance.
	evi vni-id	The specified evl instance.
Defaults	N/A	
Command		
Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays all L2VPN EVPN address family routing information. <pre> FS(config)# show bgp l2vpn evpn all BGP table version is 16, local router ID is 1.1.1.1 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale, b - backup entry Origin codes: i - IGP, e - EGP, ? - incomplete Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 1:100 (Default for EVI 1122) *> 0:32:1.1.1.1/72 0.0.0.0 32768 i Total number of prefixes 1 Route Distinguisher: 1.1.1.1:100 (Default for EVI 100) *> 0:6:0011.2233.2016:0:0.0.0/128 0.0.0.0 32768 i *> i0:6:00d0.f822.33df:0:0.0.0/128 2.2.2.2 0 100 0 i *> 0:6:0011.2233.2016:32:100.1.1.2/128 0.0.0.0 32768 i *> i0:6:00d0.f822.33df:32:100.1.1.1/128 2.2.2.2 0 100 0 i *> 0:32:1.1.1.1/72 0.0.0.0 32768 i *> i0:32:2.2.2.2/72 2.2.2.2 0 100 0 i Total number of prefixes 6 </pre>	

	Command	Description
	BGP table version	BGP table version.
	Local Router ID	Local Router ID. Generally it is a loopback address.
	status codes	Status codes: s :The route is dampened. d :Shielded route flap. h: Historical routes that no longer available * : Valid routes > : Optimal routes i : IGBP routes r : Fails to install the RIB routing table. S: Old routes.
	Origin Codes	Origin Codes: i: IGP. e: EGP. ?: Incomplete.
	Network	Routing information in the form aa:bb. The aa here represents site ID and the bb represents label model offset.
	Next hop	Next hop IP address.
	Metric	Metric value of the represent route (if be displayed.)
	LocPrf	Local priority.
	Path	AS path that reach the destination network.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.147 show bgp l2vpn update-group

	Use this command to display the update-group information of BGP L2VPN address family. show bgp l2vpn { evpn } all update-group [neighbor-address update-group-index] [summary]	
Parameter Description	Parameter	Description
	evpn	Displays the L2VPN EVPN address family information.
	<i>neighbor-address</i>	Displays the update-group information of specified neighbor.
	<i>update-group-index</i>	Display the specified update-group information.
	summary	Display neighbor information.
Defaults	N/A	

Command																															
Mode	Privileged EXEC mode																														
Usage Guide	Display the update-group information of BGP L2VPN address family.																														
Configuration Examples	The following example displays the update-group information of BGP L2VPN EVPN address family																														
	<pre>FS#show bgp l2vpn evpn all update-group BGP version 4 update-group 1(ref 2), internal, Address Family: L2VPN EVPN Update message formatted 2, replicated 2 Minimum route advertisement interval is 0 seconds Minimum AS origination interval is 1 seconds Format state: Current working Refresh blocked Has 1 members: 192.168.195.183</pre>																														
	The following example displays the neighbor summay of update-group 1 of BGP L2VPN EVPN address family																														
	<pre>FS # show bgp l2vpn evpn all update-group 1 summary BGP router identifier 192.168.183.1, local AS number 23 BGP table version is 2 2 BGP AS-PATH entries 1 BGP community entries</pre> <table><tr><td>Neighbor</td><td>V</td><td>AS</td><td>MsgRcvd</td><td>MsgSent</td><td>TblVer</td><td>InQ</td><td>OutQ</td><td>Up/Down</td><td>State/PfxRcd</td></tr><tr><td>192.168.195.79</td><td>4</td><td>24</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>never</td><td>Active</td></tr><tr><td>192.168.195.183</td><td>4</td><td>23</td><td>17</td><td>15</td><td>1</td><td>0</td><td>0</td><td>00:09:04</td><td>8</td></tr></table> <pre>Total number of neighbors 2</pre>	Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd	192.168.195.79	4	24	0	0	0	0	0	never	Active	192.168.195.183	4	23	17	15	1	0	0	00:09:04	8
	Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd																					
192.168.195.79	4	24	0	0	0	0	0	never	Active																						
192.168.195.183	4	23	17	15	1	0	0	00:09:04	8																						
<table><tr><th>Field</th><th>Description</th></tr><tr><td>BGP router identifier</td><td>BGP router ID</td></tr><tr><td>local AS number</td><td>Local AS number of BGP</td></tr><tr><td>BGP table version</td><td>Version of the BGP routing table</td></tr><tr><td>BGP AS-PATH entries</td><td>Number of AS path entries</td></tr><tr><td>BGP community entries</td><td>Number of community attribute entries</td></tr><tr><td>Neighbor</td><td>Peer address</td></tr><tr><td>V</td><td>Protocol version</td></tr><tr><td>AS</td><td>Peer AS number</td></tr><tr><td>MsgRcvd</td><td>Number of received packets</td></tr><tr><td>MsgSent</td><td>Number of sent packets</td></tr><tr><td>State/PfxRcd</td><td>Status of the neighbor state machine or number of received routing entries</td></tr></table>	Field	Description	BGP router identifier	BGP router ID	local AS number	Local AS number of BGP	BGP table version	Version of the BGP routing table	BGP AS-PATH entries	Number of AS path entries	BGP community entries	Number of community attribute entries	Neighbor	Peer address	V	Protocol version	AS	Peer AS number	MsgRcvd	Number of received packets	MsgSent	Number of sent packets	State/PfxRcd	Status of the neighbor state machine or number of received routing entries							
Field	Description																														
BGP router identifier	BGP router ID																														
local AS number	Local AS number of BGP																														
BGP table version	Version of the BGP routing table																														
BGP AS-PATH entries	Number of AS path entries																														
BGP community entries	Number of community attribute entries																														
Neighbor	Peer address																														
V	Protocol version																														
AS	Peer AS number																														
MsgRcvd	Number of received packets																														
MsgSent	Number of sent packets																														
State/PfxRcd	Status of the neighbor state machine or number of received routing entries																														
Platform																															
Description	N/A																														

5.148 show bgp statistics

	Use this command to display the BGP statistics information. <pre>show bgp statistics [vrf vrf-name]</pre>

Parameter	Parameter	Description
Description	vrf vrf-name	Displays the BGP statistics information of VRF.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Without the vrf parameter, the global BGP statistics information will be displayed.	
Configuration Examples	The following example displays the BGP statistics information.	
	FS#show bgp statistics	
	Local as 100, Router id 1.1.1.1	
	Total neighbor 10, Established neighbor 9, Admin-Down neighbor 1	
	IBGP neighbor 8, Established IBGP neighbor 8, Admin-Down IBGP neighbor 0	
	EBGP neighbor 2, Established EBGp neighbor 1, Admin-Down EBGp neighbor 1	
	AS-PATH entries 1, Community entries 1, Extended-Community entries 0	
	For address family: IPv4 Unicast	
	Activated neighbor 9, Unactivated neighbor 0	
	Activated IBGP neighbor 8, Unactivated IBGP neighbor 0	
	Activated EBGp neighbor 1, Unactivated EBGp neighbor 0	
	For address family: IPv6 Unicast	
	Activated neighbor 0, Unactivated neighbor 9	
	Activated IBGP neighbor 0, Unactivated IBGP neighbor 0	
	Activated EBGp neighbor 0, Unactivated EBGp neighbor 0	
		Parameter
	Router id	ID of BGP router.
	Total neighbor	Total number of neighbors.
	Established neighbor	Number of UP neighbors.
	Admin-Down neighbor	Number of admin down neighbors.
	IBGP neighbor	Number of IBGP neighbors.
	Established IBGP neighbor	Number of UP IBGP neighbors.
	Admin-Down IBGP neighbor	Number of admin down IBGP neighbors.
	EBGP neighbor	Number of EBGp neighbors.
	AS-PATH entries	Number of AS-PATH entries.
	Community entries	Number of community entries.
	Extended-Community	Number of extended community entries.
	Established EBGp neighbor	Number of UP EBGp neighbors.
	Admin-Down EBGp neighbor	Number of admin down EBGp neighbors.
	Activated neighbor	Number of activated neighbors.
	Unactivated neighbor	Number of unactivated neighbors, not including UP neighbors.
	Activated IBGP neighbor	Number of activated IBGP neighbors.

	Unactivated IBGP neighbor	Number of unactivated IBGP neighbors, not including UP neighbors.
	Activated EBGp neighbor	Number of activated EBGp neighbors.
	Unactivated EBGp neighbor	Number of unactivated EBGp neighbors, not including UP neighbors.
Platform Description	N/A	

5.149 show evpn

	Use this command to display the EVI instance. show evpn [vni-id [detail] detail]		
Parameter	Parameter	Description	
Description	vni-id	Indicates the ID of specified EVI instance.	
Defaults	N/A		
Command Mode	Privileged EXEC mode		
Usage Guide	If an ID of EVI instance is exported, display the information of the EVI. IF no EVI ID is imported, display all EVIs' information.		
Configuration Examples	The following example displays all information of EVI 100.		
	FS#show evpn 100 detail		
	EVI 100, RD 1.1.1.1:100(auto)		
	Import VPN route-target communities		
	RT: 100:100(auto)		
	Export VPN route-target communities		
	RT: 100:100(auto)		
	EVI Layer 3 Interface: OverlayRouter 100		
	All Route count: 6		
Ethernet Auto-discovery Route count: 0			
MAC/IP Advertisement Route count: 4			
Inclusive Multicast Ethernet Tag Route count: 2			
Ethernet Segment Route count: 0			
Install Route count: 3			
	Parameter	Description	
	RD	RD value of EVI.	
	EVI Layer 3 Interface	L3 interface associated with EVI.	
	Export VPN route-target communities	Value of the exported RT of EVI.	
	Import VPN route-target	Value of the imported RT of EVI.	

	communities		
	Route count		Number of routes in EVI instance.
	The following example displays key information of EVI.		
	FS#show evpn		
	vni	rd	interface
	100	1.1.1.1:100	OverlayRouter 100
	300	1.1.1.1:300	N/A
	789	1.1.1.1:789	N/A
	1000	1.1.1.1:1000	OverlayRouter 1000
	1122	1:100	N/A
2000	1.1.1.1:2000	OverlayRouter 2000	
3344	1.1.1.1:3344	N/A	
1678889	1.1.1.1:40489	N/A	
Total number: 8			
	Parameter	Description	
	vni	vni-id of EVI.	
	rd	RD value of EVI	
	interface	L3 interface associated with EVI.	
Related	Command		Description
Commands	N/A		N/A
Platform			
Description	N/A		

5.150 show evpn mac

	Use this command to display the mobilized or conflict MAC information show evpn mac {conflict mobility} [vni-id]			
Parameter	Parameter	Description		
Description	conflict	Display the conflicted MAC		
	mobility	Display the mobilized MAC		
	vni-id	Display the ID of specific EVI instance		
Defaults	N/A			
Command Mode	Privileged EXEC mode			
Usage Guide	If the parameter has EVI ID, then display the MAC information of specific EVI; if no EVI ID is entered, display the MAC information of all EVI.			
Configuration Examples	The following example checks the mobilized MAC information. FS#show evpn mac mobility vni mac count remain-time 10 0055.1000.0004 2 72 10 0055.1000.000a 1 66			

	10	0055.1000.000e	1	72								
	10	0055.1000.0013	1	27								
	10	0055.1000.0015	4	75								
	Parameter		Description									
	vni		VNI-ID of EVI.									
	mac		Mobilized MAC address									
	count		Mobility times									
	remain-time		Remaining time of the timer for conflict. Unit: second.									
The following example checks the conflict MAC information.												
FS#show evpn mac conflict FS#show evpn mac conflict <table><tr><td>vni</td><td>mac</td><td>seq</td><td>retry-time</td></tr><tr><td>10</td><td>0011.0011.e69c</td><td>6</td><td>-</td></tr></table>					vni	mac	seq	retry-time	10	0011.0011.e69c	6	-
vni	mac	seq	retry-time									
10	0011.0011.e69c	6	-									
Parameter		Description										
vni		vni-id of EVI.										
mac		Mobilized MAC address										
seq		Sequence number of conflict MAC address										
Retry-time		Remaining time for retry. Unit: second										
Related Commands	Command		Description									
	N/A		N/A									
Platform Description	N/A											

5.151 show ip bgp

	Use this command to display the BGP IPv4 unicast address families' route information. The method of use is the same as other BGP show commands.
	show ip bgp [vrf <i>vrf-name</i>] [<i>network</i> [<i>network-mask</i> [longer-prefixes]]] cidr-only community [<i>community-number</i> [exact-match]] filter-list <i>path-list-number</i> community-list <i>community-name</i> [exact-match] regex <i>regex</i> quote-regex <i>regex</i> extcommunity-list <i>extcommunity-name</i> inconsistent-as prefix-list <i>ip-prefix-list-name</i> route-map <i>map-tag</i>]
	Display route flap's parameters.
	show ip bgp [vrf <i>vrf-name</i>] dampening { flap-statistics dampened-paths parameters }
	Display neighbors' related information.
	show ip bgp [vrf <i>vrf-name</i>] neighbors [<i>peer-address</i> [received-routes routes advertised-routes [policy [detail]]]]
	show ip bgp [vrf <i>vrf-name</i>] summary
	Display directory information.
	show ip bgp [vrf <i>vrf-name</i>] paths Display route scan status.
	show ip bgp scan

	Display related information under VRF.	
	show ip bgp { vrf vrf-name labels } Display related information of BGP IPv4 unicast update-group. show ip bgp [vrf vrf-name] update-group [neighbor-address update-group-index] [summary]	
Parameter Description	Parameter	Description
	vrf-name	VRF name.
	network	Displays specific route information in the route table.
	network-mask	Displays route information in the specific network.
	longer-prefixes	Displays the route map information.
	cidr-only	Displays route information without specific category.
	community community-number	Displays route information containing specific community value. The <i>community-number</i> is the group number. The format is AA:NN (autonomous system number/2-byte figure), or the following pre-defined value: internet, no-export, local-as or no-advertise.
	community-list community-name	Displays the BGP route information of the specified community list. The <i>community-name</i> is the name of the community list.
	dampening dampened-paths	Displays dampened route information.
	dampening flap-statistics	Displays the route flap statistics.
	dampening parameters	Displays believed route flap parameters.
	extcommunity-list extcommunity-name	Displays route information containing specific extcommunity value.
	filter-list path-list-number	Displays the route information that complies with the filter list. The <i>path-list-number</i> is the marking number of the filter list.
	inconsistent-as	Displays the route information of inconsistent source AS.
	Labels	Displays the IPv4 label route information.
	neighbors peer-address	Displays the route information of BGP neighbors.
	neighbors peer-address received-routes	Displays all routing information received from the specified peer (including accepted and refused routes).
	neighbors peer-address routes	Displays all the routing information received from the peer and accepted.
	neighbors peer-address advertised-routes	Displays all the routing information sent to the specified peer.
	neighbors peer-address policy	Displays the related routing policy information of BGP neighbors. (General)
	neighbors peer-address policy detail	Displays the related routing policy information of BGP neighbors. (Detail)
	Paths	Displays the route information in the route database.
	prefix-list	Displays the route information that complies with the prefix list.
	quote-regexp regexp	Displays the BGP route information of regular expression in the specified double quotation mark of the AS route attribute.
	regexp regexp	Displays the BGP route information of specified regular expression of the AS route attribute.

	route-map	Displays the route information that complies with the route map.
	Scan	Displays the BGP route scanning status.
	summary	Displays related information of BGP neighbors.
	update-group [<i>neighbor-address</i> <i>update-group-index</i>]	Display update-group information. When <i>neighbor-address</i> is specified, display the update-group information of the specified neighbor. When <i>update-group-index</i> is specified, display the specified update-group information.
Defaults	-	
Command Mode	Privileged EXEC mode	
Usage Guide	The show ip bgp command is the same as show bgp ipv4 unicast in terms of the function. All the parameters in show bgp ipv4 unicast apply to show ip bgp .	
Configuration Examples	-	
Configuration Examples	Command	Description
	show bgp ipv4 unicast	Displays IPv4 unicast route information in BGP route information.
Platform Description	-	

5.152 vni

	Use this command to create an EVI instance. Use the no form of this command to delete the EVI instance. Use the default form of this command to restore the default settings. vni <i>vni-id</i> no vni <i>vni-id</i> default vni <i>vni-id</i>	
Parameter Description	Parameter	Description
	<i>vni-id</i>	Indicates the VNI ID. Ranges from 1 to 16777215.
Defaults	N/A	
Command Mode	EVPN configuration mode	

Usage Guide	Configure the EVPN mode first, and then enter the evpn-vni configuration mode. Run exit command to exit.	
Configuration Examples	The following example configures an EVI instance in EVPN mode. FS(config)# evpn FS(config-evpn)# vni 100	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.153 vni range

	Use this command to create EVI instances in batches and enter the EVI instance batch configuration mode. Use the no form of this command to delete EVI instances in batches. Use the default form of this command to restore the default settings.	
	vni range <i>vni-id-list</i>	
	no vni range <i>vni-id-list</i>	
	default vni range <i>vni-id-list</i>	
Parameter	Parameter	Description
Description	<i>vni-id-list</i>	Name of the VNI ID list
Defaults	N/A	
Command Mode	EVPN configuration mode.	
Default Level	14	
Usage Guide	✔ The configuration fails if the number of configured VNI instances exceeds the capacity or a VNI instance is being deleted. ✔ The RD values of different VNI instances must be different. Therefore, only the automatic RD configuration mode is available for configuring VNI instances in batches, and VNI instances cannot be configured manually.	
Configuration Examples	The following example configures EVI instances in batches in EVPN configuration mode. FS(config)# evpn FS(config-evpn)# vni range 100,200-300 FS(config-evpn-vni-range)#	
Verification	Run the show running-config command to display the EVPN configurations.	

Prompts	1. The following error information is displayed if the number of VNI instances exceeds the capacity. % this range configuration may beyond vni capacity(8000). please check your input
	2. The following error information is displayed if a VNI instance is being deleted. % evpn evi 100 is deleting, Fail to configure vni range.

6 PBR Commands

6.1 clear ip pbr statistics

	Use this command to clear the IPv4 PBR forwarded packet count.	
	clear ip pbr statistics [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the device clears the IPv4 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv4 PBR forwarded packet count on every interface where IPv4 PBR is enabled.
	local	Clears the IPv4 PBR forwarded packet count on the local interface.
Command Mode	Privileged EXEC mode.	
Usage Guide	Use this command to clear the IPv4 PBR forwarded packet count.	
Configuration Examples	The following example clears the IPv4 PBR forwarded packet count.	
	FS#clear ip pbr statistics	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.2 clear ipv6 pbr statistics

	Use this command to clear the IPv6 PBR forwarded packet count.	
	clear ipv6 pbr statistics [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the device clears the IPv6 PBR forwarded packet count on that interface. Otherwise, the device clears the IPv6 PBR forwarded packet count on every interface where IPv6 PBR is enabled.
	local	Clears the IPv6 PBR forwarded packet count on the local interface.
Defaults	N/A	

Command Mode	Privileged EXEC mode.				
Usage Guide	Use this command to clear the IPv6 PBR forwarded packet count.				
Configuration Examples	The following example clears the IPv6 PBR forwarded packet count. FS#clear ipv6 pbr statistics				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.3 ip local policy route-map

	Use this command to apply the policy-based routing (PBR) on the packets sent locally. Use the no form of this command to restore the default setting.	
	ip local policy route-map <i>route-map</i>	
	no ip local policy route-map	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	Name of the route map
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. The set interface command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.	
Configuration Examples	The following examples send the packets with the source address 192.168.217.10 from the serial 2/0. The following example defines an ACL that match the IP packet. FS(config)#access-list 1 permit 192.168.217.10	

	The following example defines the route map. <pre>FS(config)#route-map lab1 permit 10 FS(config-route-map)#match ip address 1 FS(config-route-map)#set interface serial 2/0 FS(config-route-map)#exit</pre> The following example applies PBR on the local interface. <pre>FS(config)#ip local policy route-map lab1</pre>	
Related Commands	Command	Description
	access-list	Defines the access list rule.
	route-map	Defines the route map.
	set vrf	Defines the VRF instance of the policy-based IP packet.
	set ip next-hop	Defines the next hop of the policy-based routing.
	set ip default next-hop	Defines the default next hop of the policy-based routing.
	set interface	Defines the output port of the policy-based routing.
	set default interface	Defines the default policy-based routing output port.
	set ip tos	Sets the TOS in the head of the IP packet.
	set ip dscp	Sets the DSCP of the IP packet.
	set ip precedence	Sets the priority level in the head of the IP packet.
	match ip address	Sets the filtering rule.
	match length	Matches the packet length.
Platform Description	N/A	

6.4 ip policy

	Use this command to set the policy: redundant backup or load balancing used between multiple next hops of the PBR applied for the set ip [default] nexthop command in global configuration mode. Use the no form of this command to restore the default setting.	
	ip policy { load-balance redundancy }	
	no ip policy	
Parameter Description	Parameter	Description
	load-balance redundancy	Specifies the policy: load balancing or redundant backup.
Defaults	Redundant backup is adopted by default.	
Command	Global configuration mode	

Mode						
Usage Guide	When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop of the policy-based routing takes effect. When the load balancing is set, multiple resolved next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops. The resolved next hop refers to the ARP message learned by the next hop and the MAC address corresponding to this ARP exists in the MAC address table.  NPE80 does not support this command.					
Configuration Examples	In the example below, there are multiple next hops configured in the route map. After the redundant backup is set in global configuration mode, only the first next hop among the sub-route map of the policy-based routing applied on the interface FastEthernet 0/0 takes effect. The following example sets the ACL that match the IP packet. <pre>FS(config)#access-list 1 permit 10.0.0.1 FS(config)#access-list 2 permit 20.0.0.1</pre> The following example defines the route map. <pre>FS(config)#route-map lab1 permit 10 FS(config-route-map)#match ip address 1 FS(config-route-map)#set ip next-hop 196.168.4.6 FS(config-route-map)#set ip next-hop 196.168.4.7 FS(config-route-map)#set ip next-hop 196.168.4.8 FS(config-route-map)#exit FS(config)#route-map lab1 permit 20 FS(config-route-map)#match ip address 2 FS(config-route-map)#set ip next-hop 196.168.5.6 FS(config-route-map)#set ip next-hop 196.168.5.7 FS(config-route-map)#set ip next-hop 196.168.5.8 FS(config-route-map)#exit</pre> The following example applies the policy-based routing on the interface. <pre>FS(config)#interface FastEthernet 0/0 FS(config-if)#ip policy route-map lab1 FS(config-if)#exit FS(config)#ip policy redundancy</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

6.5 ip policy route-map

	Use this command to apply the policy-based routing on an interface. Use the no form of this command to restore the default setting.	
	ip policy route-map <i>route-map</i>	
	no ip policy route-map	
Parameter Description	Parameter	Description
	<i>route-map</i>	Name of the route map
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.  Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.	
Configuration Examples	In the example below, when the interface FastEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.1, it sets the next-hop as 196.168.4.6; if the source address is 20.0.0.1, it sets the next-hop as 196.168.5.6; otherwise, the general forwarding will be performed. The following example sets the ACL matched with the IP packets. <pre>FS(config)#access-list 1 permit 10.0.0.1 FS(config)#access-list 2 permit 20.0.0.1</pre> The following example defines the route map. <pre>FS(config)#route-map lab1 permit 10 FS (config-route-map)#match ip address 1 FS(config-route-map)#set ip next-hop 196.168.4.6 FS(config-route-map)#exit FS(config)#route-map lab1 permit 20 FS(config-route-map)#match ip address 2 FS(config-route-map)#set ip next-hop 196.168.5.6 FS(config-route-map)#exit</pre> The following example applies the route map on the interface. <pre>FS(config)#interface FastEthernet 0/0</pre>	

	<pre>FS(config-if)#ip policy route-map lab1 FS(config-if)#exit</pre>	
Related Commands	Command	Description
	access-list	Defines the access list rule.
	route-map	Defines the route map.
	set vrf	Defines the VRF instance of the policy-based IP packet.
	set ip next-hop	Defines the next hop of the policy-based routing.
	set ip default next-hop	Defines the default next hop of the policy-based routing.
	set interface	Defines the policy-based routing output port.
	set default interface	Defines the default policy-based routing output port.
	set ip tos	Sets the TOS in the head of the IP packet.
	set ip dscp	Sets the DSCP of the IP packet.
	set ip precedence	Sets the priority level in the head of the IP packet.
	match ip address	Sets the filtering rule.
	match length	Matches the packet length.
Platform Description	N/A	

6.6 ip policy-source in-interface

	Use this command to configure the source address policy-based routing for the IPv4 packets received on an interface. Use the no form of this command to disable the source address policy-based routing on the interface.	
	<pre>ip policy-source in-interface interface-type sequence { source-address mask source-address/mask } [[default] next-hop ip-address [weight] [default] interface out-interface-type vrf vrf-name]</pre>	
	<pre>no ip policy-source in-interface interface-type sequence [{ source-address mask source-address/mask } [[default] next-hop ip-address [weight] [default] interface out-interface-type vrf vrf-name]]</pre>	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>sequence</i>	Policy sequence number. The lower the number is, the higher the priority is.
	<i>source-address</i>	Source IPv4 address.
	<i>mask</i>	Address mask.
	<i>ip-address</i>	Next hop IPv4 address
	<i>weight</i>	Next hop weight
	<i>out-interface-type</i>	Type of the next hop interface
	<i>vrf-name</i>	VRF instance name
Defaults	Source address policy-based routing is disabled by default.	

Command Mode	Global configuration mode				
Usage Guide	You can configure multiple ip source-policy in-interface commands on an interface. The policy with different source addresses must be configured with different sequence numbers. The lower the sequence number is, the higher the priority is. In case of the same sequence number, the priority order of the next hop type is as follows: vrf <i>vrf-name</i> > next-hop <i>ip-address</i> > interface <i>out-interface-type</i> > default next-hop <i>ip-address</i> > default interface <i>out-interface-type</i> The priority of the source address PBR is lower than that of the interface PBR.				
Configuration Examples	In the example below, when the interface GigabitEthernet0/0 receives a datagram, if the source address of the datagram is 10.0.0.2, the next-hop is set as 196.168.1.2; otherwise, the general forwarding will be performed. The following example configures source address PBR in global configuration mode. <pre>FS(config)# ip source-policy in-interface gigabitEthernet 0/0 1 10.0.0.2 255.255.255.255 next-hop 196.168.1.2 FS(config)# ip source-policy in-interface gigabitEthernet 0/0 2 20.0.0.2 255.255.255.255 next-hop 196.168.2.2</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

6.7 ipv6 local policy route-map

	Use this command to enable the policy-based routing on the packets sent locally. Use the no form of this command to restore the default setting.	
	ipv6 local policy route-map <i>route-map-name</i>	
	no ipv6 local policy route-map	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	Name of the router map applied locally, which is configured by the router-map command.
Defaults	This function is disabled by default.	
Command Mode	Global Configuration mode	
Usage Guide	- This command is valid only for the IPv6 packets in accordance with the policy (for example, ping packets used for management) sent locally, but not the packets received locally. - To use the policy-based routing, you must specify the route map for it and create the route map. A route	

	map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.	
Configuration Examples	The following examples display the PBR application process: The device sends the packets from the source address 2003:1000::10/80 to the 2001:100::/64, the packets will match ACL6 of aaa and be sent to the device 2003:1001::2. - The following example defines the ACL matched with the IPv6 packet: <pre>FS(config)#ipv6 access-list aaa FS(config)#permit ipv6 2003:1000::10/80 2001:100::/64</pre> - The following example defines the router map. <pre>FS(config)#route-map pbr-aaa permit 10 FS(config-route-map)#match ipv6 address aaa FS(config-route-map)#set ipv6 next-hop 2003::1001::2</pre> - The following example applies the PBR on the device. <pre>FS(config)#ipv6 local policy route-map pbr-aaa</pre>	
Related Commands	Command	Description
	match ipv6 address	Sets the ACL6 used to match the IPv6 packets in the IPv6 PBR.
	match length	Defines the length of matched packets.
	route-map	Defines the route map for PBR.
	set default interface	Defines the default next hop output port.
	set interface	Defines the next hop output port.
	set ipv6 default next-hop	Sets the default next hop of packet forwarding.
	set ipv6 next-hop	Sets the next hop of packet forwarding.
	set ipv6 precedence	Sets the priority field in the head of IPv6 packets.
	show ipv6 policy	Displays the current PBR application.
	show route-map	Displays the current router map configuration.
Platform Description	N/A	

6.8 ipv6 policy

	Use this command to set the policy: redundant backup or load balancing, applied for the set ip nexthop command in global configuration mode. Use the no form of this command to restore the default setting.
	ipv6 policy { load-balance redundancy }
	no ipv6 policy

Parameter Description	Parameter	Description
	load-balance	Sets the policy as load balancing.
	redundance	Sets the policy as redundant backup.
Defaults	Redundant backup is adopted by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is valid for the IP packets sent locally, but not the IP packets received locally. The IP packets received by the local are free from this command. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. The set interface command for the policy-based routing does not support the load-balancing and only supports the redundancy backup.	
Configuration Examples	This function is valid for the multiple next-hops. When you configure the set ip next-hop command in sub-route map, it is possible to configure multiple next hops. However, when you set redundant backup, only the first resolved next hop takes effect. The second configured next hop will take effect only when the first one fails and the first next hop will take effect again if it recovers. When the load balancing is set, multiple next hops of the policy-based routing take effect. The WCMP can be set up to 8 next hops, and the ECMP can be set up to 32 next hops.  The resolved next hop refers to the learned MAC address for the next-hop. The following example sets load-balancing mode for multiple nexthops. The following example configures an ACL matching with IP packets. <pre> FS(config)# ipv6 access-list 1 FS(config-ipv6-acl)# permit ipv6 1000::1 any FS(config)# ipv6 access-list 2 FS(config-ipv6-acl)# permit ipv6 2000::1 any </pre> The following example defines a route map. <pre> FS(config)# route-map lab1 permit 10 FS(config-route-map)# match ipv6 address 1 FS(config-route-map)# set ipv6 next-hop 2002::1 FS(config-route-map)# set ipv6 next-hop 2002::2 FS(config-route-map)# set ipv6 next-hop 2002::3 FS(config-route-map)# exit FS(config)# route-map lab1 permit 20 FS(config-route-map)# match ipv6 address 2 </pre>	

	<pre>FS(config-route-map)# set ipv6 next-hop 2002::5 FS(config-route-map)# set ipv6 next-hop 2002::6 FS(config-route-map)# set ipv6 next-hop 2002::7 FS(config-route-map)# exit</pre> The following example applies policy-based routing on the interface. <pre>FS(config)# interface FastEthernet 0/0 FS(config-if)# ipv6 policy route-map lab1 FS(config-if)# exit FS(config)# ipv6 policy load-balance</pre>	
Related Commands	Command	Description
	set ipv6 default next-hop	Defines the default next hop for forwarding the packets.
	set ipv6 next-hop	Defines the next hop for forwarding the packets.
	show ipv6 policy	Displays the current policy-based routing application.
Platform Description	N/A	

6.9 ipv6 policy route-map

	Use this command to apply the policy-based routing on an interface in interface configuration mode. Use the no form of this command to restore the default setting. ipv6 policy route-map <i>route-map-name</i>	
	no ip policy route-map	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	Name of the PBR router map applied locally, which is configured by the router-map command.
Defaults	This function is disabled by default..	
Command Mode	Interface configuration mode	
Usage Guide	The policy-based routing must be applied on the specified interface. That interface performs the policy-based routing only on the received packets. To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.	



Up to one route map can be configured on an interface. When you configure a route map on the interface for many times, the latter will overwrite the former.

Configuration Examples	An IPv6 packet is received on the fastEthernet 0/0. If the packet is sent from 10::/64 network segment, it is forwarded to the next hop of 2000:1; if the packet is sent from 20::/64 network segment, it is forwarded to the next hop of 2000:2 or forwarded as usual.: The following example configures an ACL matched with the IP packet. <pre>FS(config)# ipv6 access-list acl_for_pbr1 FS (config-ipv6-acl)# permit ipv6 10::/64 any FS(config)# ipv6 access-list acl_for_pbr2 FS (config-ipv6-acl)# permit ipv6 20::/64 any</pre> The following example defines a route map. <pre>FS(config)# route-map rm_pbr permit 10 FS (config-route-map)# match ipv6 address acl_for_pbr1 FS(config-route-map)# set ipv6 next-hop 2000::1 FS(config-route-map)# exit FS(config)# route-map rm_pbr permit 20 FS(config-route-map)# match ipv6 address acl_for_pbr2 FS(config-route-map)# set ipv6 next-hop 2000::2 FS(config-route-map)# exit</pre> The following example applies the route map to the interface. <pre>FS(config)# interface FastEthernet 0/0 FS(config-if)# no switchport FS(config-if)# ipv6 policy route-map rm_pbr FS(config-if)# exit</pre>	
Related Commands	Command	Description
	route-map	Defines the route map.
	match ipv6 address	Sets the IPv6 ACL used to match the IPv6 packets in the IPv6 PBR.
	set ipv6 default next-hop	Defines the default next hop of the packet forwarding.
	set ipv6 next-hop	Defines the next hop of the packet forwarding.
	show ipv6 policy	Displays the current policy-based routing application.
	show route-map	Displays the current route map configurations.
Platform Description	N/A	

6.10 ipv6 policy-source in-interface

	Use this command to configure the source address policy-based routing for the IPv6 packets received on an interface. Use the no form of this command to disable the source address policy-based routing on the interface.	
	ipv6 policy-source in-interface <i>interface-type</i> <i>sequence</i> <i>source-address/prefix-length</i> {[default] next-hop <i>ipv6-address</i> [<i>weight</i>] } [default] interface <i>out-interface-type</i> vrf <i>vrf-name</i> }	
	no ipv6 policy-source in-interface <i>interface-type</i> <i>sequence</i> [<i>source-address/prefix-length</i> [[default] next-hop <i>ipv6-address</i> [<i>weight</i>]] [default] interface <i>out-interface-type</i> vrf <i>vrf-name</i> }	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>sequence</i>	Policy sequence number. The lower the number is, the higher the priority is.
	<i>source-address</i>	Source IPv6 address.
	<i>ipv6-address</i>	Next hop IPv6 address
	<i>weight</i>	Next hop weight
	<i>out-interface-type</i>	Type of the next hop interface
	<i>vrf-name</i>	VRF instance name
Defaults	Source address PBR is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	You can configure multiple ipv6 source-policy in-interface commands on an interface. The policy with different source addresses must be configured with different sequence numbers. The lower the sequence number is, the higher the priority is. In case of the same sequence number, the priority order of the next hop type is as follows: vrf <i>vrf-name</i> > next-hop <i>ipv6-address</i> > interface <i>out-interface-type</i> > default next-hop <i>ipv6-address</i> > default interface <i>out-interface-type</i> The priority of the source address PBR is lower than that of the interface PBR.	
Configuration Examples	In the example below, when the interface GigabitEthernet0/0 receives an IPv6 datagram, if the source address of the datagram is in the network segment of 10::/64, the next-hop is set as 2000:1; if the source address of the datagram is in the network segment of 20::/64, the next-hop is set as 2000:2; otherwise, the general forwarding will be performed. The following example configures source address PBR in global configuration mode. <pre>FS(config)# ipv6 source-policy in-interface gigabitEthernet 0/0 2 10::/64 next-hop 2000:1 FS(config)# ipv6 source-policy in-interface gigabitEthernet 0/0 2 20::/64 next-hop 2000:2</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

6.11 show ip pbr bfd

	Use this command to display the correlation between the IPv4 policy router and BFD.																										
	show ip pbr bfd																										
Parameter Description	Parameter		Description																								
	N/A		N/A																								
Defaults	N/A																										
Command Mode	Privileged EXEC mode																										
Usage Guide	N/A																										
Configuration Examples	The following example displays the correlation between the IPv4 policy router and BFD. <pre>FS# show ip pbr bfd</pre> <table><thead><tr><th>VRF ID</th><th>Ifindex</th><th>Host</th><th>State</th><th>Refcnt</th></tr></thead><tbody><tr><td>0</td><td>13</td><td>192.168.8.100</td><td>Up</td><td>2</td></tr></tbody></table> Field Description <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>VRF ID</td><td>VRF of BFD neighbors correlated with the policy router</td></tr><tr><td>Ifindex</td><td>The interface index of BFD neighbors correlated with the policy router</td></tr><tr><td>Host</td><td>The peer IPv4 address</td></tr><tr><td>State</td><td>Up/Down status of BFD neighbors correlated with the policy router</td></tr><tr><td>Refcnt</td><td>Calculation referred by BFD neighbors</td></tr></tbody></table>					VRF ID	Ifindex	Host	State	Refcnt	0	13	192.168.8.100	Up	2	Field	Description	VRF ID	VRF of BFD neighbors correlated with the policy router	Ifindex	The interface index of BFD neighbors correlated with the policy router	Host	The peer IPv4 address	State	Up/Down status of BFD neighbors correlated with the policy router	Refcnt	Calculation referred by BFD neighbors
VRF ID	Ifindex	Host	State	Refcnt																							
0	13	192.168.8.100	Up	2																							
Field	Description																										
VRF ID	VRF of BFD neighbors correlated with the policy router																										
Ifindex	The interface index of BFD neighbors correlated with the policy router																										
Host	The peer IPv4 address																										
State	Up/Down status of BFD neighbors correlated with the policy router																										
Refcnt	Calculation referred by BFD neighbors																										
Related Commands	Command		Description																								
	N/A		N/A																								
Platform Description	N/A																										

6.12 show ip pbr route

	Use this command to display the IPv4 PBR information on the interface.	
	show ip pbr route [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 BPR information of this interface is displayed. Otherwise, the IPv4 BPR information of all interfaces where the IPv4 PBR is enabled is displayed.
	local	Displays the IPv4 PBR information on the local interface
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to display the IPv4 PBR information.	
Configuration Examples	The following example displays the IPv4 PBR information on the interfaces. <pre> FS#show ip pbr route PBR IPv4 Route Summay : 1 Interface : GigabitEthernet 0/1 Sequence : 10 ACL[0] : 2900 ACL_CLS[0] : 0 Min Length : None Max Length : None VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Tos_Dscp : None Precedence : None Tos_Dscp : 0 Precedence : 0 Mode : redundance Nexthop Count : 1 Nexthop[0] : 192.168.8.100 Weight[0] : 1 Ifindex[0] : 2 </pre>	

	Parameter	Description
	PBR IPv4 Route Summay	IPv4 PBR route count.
	Interface	Interface where IPv4 PBR is enabled.
	Sequence	The PBR serial number.
	ACL	The ACL ID used in the match rule.
	ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
	Min Length	The minimum match length.
	Max Length	The maximum match length.
	VRF ID	Port-correlated VRF ID.
	Route Flags	PBR flag bit: Route Type: "PBR" indicates PBR routes. "Normal" indicates common routes. Direct: PBR matching action, permit or deny Priority: PBR priority, High or Low Tos_Dscp: Displays whether the tos rule or the dscp rule is configured. Precedence: Displays whether the set ip precedence rule is configured.
	Mode	Specifies the redundancy mode or the next hop load balancing mode.
	Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
	Nexthop	Specifies the next hop IP address.
	Weight	Specifies the next hop weight.
	Ifindex	Specifies the outbound interface index corresponding to the next hop.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.13 show ip pbr route-map

	Use this command to display the IPv4 PBR route-map information.	
	show ip pbr route-map <i>route-map-name</i>	
Parameter Description		
	Parameter	Description
	<i>route-map-name</i>	The route-map name.

Defaults	N/A																
Command Mode	Privileged EXEC mode																
Usage Guide	N/A																
Configuration Examples	The following example displays the IPv4 PBR route-map information. <pre> FS#show ip pbr route-map rm Pbr VRF: GLOBAL, ID: 0 Forward Mode: redundance Forwarding: On route-map rm route-map index: sequence 10, permit Match rule: ACL ID : 0, ACL CLS: 0, Name: acl1 Set rule: IPv4 Nexthop: 192.168.8.100, (VRF Name: , ID: 0), Weight: 0, Flags: 0 PBR state info ifx: GigabitEthernet 0/1, Connected: true, Track State: Up </pre> <table border="1"> <thead> <tr> <th>Field</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Pbr VRF</td><td>VRF name and VRF ID.</td></tr> <tr> <td>Forward Mode</td><td>Sets the load balance mode or the redundancy mode for the next hop.</td></tr> <tr> <td>Forwarding</td><td>Displays whether the IP route forwarding is enabled.</td></tr> <tr> <td>Route-map index</td><td>The serial number and the type of the sub-map.</td></tr> <tr> <td>Match rule</td><td>Match rule.</td></tr> <tr> <td>Set rule</td><td>Set rule.</td></tr> <tr> <td>PBR state info</td><td>PBR private data information, such as outbound interface and the link state of the next hop.</td></tr> </tbody> </table>	Field	Description	Pbr VRF	VRF name and VRF ID.	Forward Mode	Sets the load balance mode or the redundancy mode for the next hop.	Forwarding	Displays whether the IP route forwarding is enabled.	Route-map index	The serial number and the type of the sub-map.	Match rule	Match rule.	Set rule	Set rule.	PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.
Field	Description																
Pbr VRF	VRF name and VRF ID.																
Forward Mode	Sets the load balance mode or the redundancy mode for the next hop.																
Forwarding	Displays whether the IP route forwarding is enabled.																
Route-map index	The serial number and the type of the sub-map.																
Match rule	Match rule.																
Set rule	Set rule.																
PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.																
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>N/A</td><td>N/A</td></tr> </tbody> </table>	Command	Description	N/A	N/A												
Command	Description																
N/A	N/A																
Platform Description	N/A																

6.14 show ip pbr source-route

	Use this command to display information about IPv4 source address-based PBR. show ip pbr source-route [interface <i>if-name</i>]

Parameter Description	Parameter	Description
	interface <i>if-name</i>	Displays the IPv4 PBR applied to a specified interface if <i>if-name</i> is specified. Displays all applied IPv4 PBR information if <i>if-name</i> is not specified.
Command Mode	Privileged EXEC mode	
Default Level	14	
Usage Guide	You can use this command to display the configured source address-based PBR.	
Configuration Examples	The following example displays information about the configured source address-based PBR. <pre>FS# show ip pbr source-route PBR IPv4 Source Route Interface : GigabitEthernet 0/1 Sequence : 10 Source address : 10.1.1.1/24 VRF ID : 0 Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundance Nexthop Count : 1 Nexthop[0] : 192.168.8.100 Weight[0] : 1 Ifindex[0] : 2</pre>	
	Field description:	
	Field	Description
	Interface	Interface to which the PBR is applied
	Sequence	Sequence number of the PBR
	VRF ID	ID of the VRF table associated with an interface
	Route Flags	Flag bit of PBR: Route Type: type of routes. The value PBR indicates PBR routes while the value Normal indicates common routes. Direct: PBR matching mode. The options include permit and deny . Priority: priority of a PBR route. The options include High and Low .

	Mode	Sets the next hop to work in redundancy mode or load balancing mode.
	Nexthop Count	Sets the number of next hops. ECMP supports a maximum of 32 next hops.
	Nexthop	Sets the next-hop IPv4 address.
	Weight	Sets the next-hop weight value.
	Ifindex	Sets the outbound interface index of the next hop.

6.15 show ip pbr statistics

	Use this command to display the IPv4 PBR forwarded packet count.	
	show ip pbr statistics [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv4 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv4 PBR forwarded packet count of all interfaces where the IPv4 PBR is enabled is displayed.
	local	Displays the IPv4 PBR forwarded packet count on the local interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the IPv4 PBR forwarded packet count. <pre>FS#show ip pbr statistics IPv4 Policy-based route statistic gigabitEthernet 0/1 statistics : 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.16 show ip policy

	Use this command to display the interface configured with the policy-based routing and the name of route map applied on the interface.

	show ip policy [<i>route-map-name</i>]	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	Indicates the name of a route map.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	You can use this command to verify the current PBR configured in the system.	
Configuration Examples	The following example displays the current PBR configured in the system. <pre>FS#show ip policy Banlance Mode: redundancy Interface Route map local test FastEthernet 0/0 test</pre>	
Related Commands	Command	Description
	ip policy route-map	Applies the policy-based routing on the interface.
	ip local policy route-map	Applies the policy-based routing on the local interface.
Platform Description	N/A	

6.17 show ipv6 pbr bfd

	Use this command to display the correlation between the IPv6 policy router and BFD.	
	show ipv6 pbr bfd	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration Examples	The following example displays the correlation between the IPv6 policy router and BFD.	
	FS# show ipv6 pbr bfd	
	VRF ID	Ifindex Host State Refcnt
	0	13 2000::2 Up 1
	Field Description	
	Field	Description
	VRF ID	VRF of BFD neighbors correlated with the policy router
	Ifindex	The interface index of BFD neighbors correlated with the policy router
	Host	The peer IPv6 address
	State	Up/Down status of BFD neighbors correlated with the policy router
Refcnt	Calculation referred by BFD neighbors	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.18 show ipv6 pbr route

	Use this command to display the IPv6 PBR information on the interface.	
	show ipv6 pbr route [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 BPR information of this interface is displayed. Otherwise, the IPv6 BPR information of all interfaces where the IPv6 PBR is enabled is displayed.
	local	Displays the IPv6 PBR information on the local interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration	The following example displays the IPv6 PBR information on the interfaces.	

Examples

```

FS#show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface          : GigabitEthernet 0/2
  Sequence         : 10
  ACL[0]           : 2901
ACL_CLS[0]         : 0
  Min Length       : None
  Max Length       : None
  VRF ID           : 0
Route Flags        :
  Route Type       : PBR
  Direct           : Permit
  Priority          : High
  Tos_Dscp         : None
  Precedence       : None
Tos_Dscp           : 0
Precedence         : 0
Mode               : redundance
Nexthop Count      : 1
  Nexthop[0]       : 10::1
  Weight[0]         : 1
  Ifindex[0]        : 3

```

Parameter	Description
PBR IPv4 Route Summay	IPv4 PBR route count.
Interface	Interface where IPv4 PBR is enabled.
Sequence	The PBR serial number.
ACL	The ACL ID used in the match rule.
ACL_CLS	The ACL type used in the match rule, such as the IP standard ACL.
Min Length	The minimum match length.
Max Length	The maximum match length.
VRF ID	Port associated VRF ID.
Route Flags	PBR flag bit: Route Type: "PBR" indicates PBR routes. "Normal" indicates common routes. Direct: PBR matching action, permit or deny Priority: PBR priority, High or Low Tos_Dscp: Displays whether the tos rule or the dscp rule is configured. Precedence: Displays whether the set ip precedence rule is configured.
Mode	Specifies the redundancy mode or the load balance mode for the next hop.

	Nexthop Count	Specifies the next hop number. ECMP supports up to 32 next hops.
	Nexthop	Specifies the next hop IP address.
	Weight	Specifies the next hop weight.
	Ifindex	Specifies the outbound interface index corresponding to the next hop
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.19 show ipv6 pbr route-map

	Use this command to display the IPv6 PBR route-map information.	
	show ipv6 pbr route-map <i>route-map-name</i>	
Parameter Description	Parameter	Description
	<i>route-map-name</i>	The route-map name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the IPv6 PBR route-map information. <pre>FS#show ipv6 pbr route-map rm6 Pbr VRF: GLOBAL, ID: 0 Forward Mode: redundance Forwarding: On route-map rm6 route-map index: sequence 10, permit Match rule: ACL ID : 0, ACL CLS: 0, Name: acl6 Set rule: IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0, Flags: 0 PBR state info ifx: GigabitEthernet 0/0, Connected: true, Track State: valid, Flags: 0</pre>	

	Field	Description
	Pbr VRF	VRF name and VRF ID.
	Forward Mode	Sets the load balancing mode or to the redundancy mode for the next hop.
	Forwarding	Displays whether the IP route forwarding is enabled.
	Route-map index	The serial number and the type of the sub-map.
	Match rule	Match rule
	Set rule	Set rule.
	PBR state info	PBR private data information, such as outbound interface and the link state of the next hop.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.20 show ipv6 pbr source- route

	Use this command to display the IPv6 source address PBR configuration.	
	show ipv6 pbr source-route [interface <i>if-name</i>]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	(Optional) Displays the IPv6 source address PBR configuration on the specified interface. If the parameter is not configured, the IPv6 source address PBR configuration on all interfaces will be displayed.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the IPv6 source address PBR configuration. <pre> FS# show ipv6 pbr source-route PBR IPv6 Source Route Interface : GigabitEthernet 0/1 Sequence : 10 Source address : 1000::1/64 VRF ID : 0 </pre>	

	Route Flags : Route Type : PBR Direct : Permit Priority : High Match_ipaddr : Exist Mode : redundancy Nexthop Count : 1 Nexthop[0] : 1001::2 Weight[0] : 1 Ifindex[0] : 3	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.21 show ipv6 pbr statistics

	Use this command to display the IPv6 PBR forwarded packet count.	
	show ip pbr statistics [interface <i>if-name</i> local]	
Parameter Description	Parameter	Description
	interface <i>if-name</i>	Specifies the interface name. If the interface name is specified, the IPv6 PBR forwarded packet count of this interface is displayed. Otherwise, the IPv6 PBR forwarded packet count of all interfaces where the IPv6 PBR is enabled is displayed.
	local	Displays the IPv6 PBR forwarded packet count on the local interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the IPv6 PBR forwarded packet count. <pre>FS#show ipv6 pbr statistics IPv6 Policy-based route statistic gigabitEthernet 0/1 statistics : 20</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

6.22 show ipv6 policy

	Use this command to display which interfaces are configured with IPv6 PBR.															
	show ipv6 policy [route-map-name]															
Parameter Description	Parameter	Description														
	route-map-name	Name of the PBR router map.														
Defaults	N/A															
Command Mode	Privileged EXEC mode															
Usage Guide	N/A															
Configuration Examples	The following example displays the current PBR applied in the system. FS#show ipv6 policy Banlance Mode: redundance <table><tr><td>Interface</td><td>Route map</td></tr><tr><td>VLAN 1</td><td>RM_for_Vlan_1</td></tr><tr><td>VLAN 2</td><td>RM_for_Vlan_2</td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Balance Mode</td><td>The current PBR running mode.</td></tr><tr><td>Interface</td><td>The name of interface with PBR applied.</td></tr><tr><td>Route map</td><td>The name of route map applied on the interface.</td></tr></table>		Interface	Route map	VLAN 1	RM_for_Vlan_1	VLAN 2	RM_for_Vlan_2	Field	Description	Balance Mode	The current PBR running mode.	Interface	The name of interface with PBR applied.	Route map	The name of route map applied on the interface.
Interface	Route map															
VLAN 1	RM_for_Vlan_1															
VLAN 2	RM_for_Vlan_2															
Field	Description															
Balance Mode	The current PBR running mode.															
Interface	The name of interface with PBR applied.															
Route map	The name of route map applied on the interface.															
Related Commands	Command	Description														
	show route-map	Displays the current configured route map.														
Platform Description	N/A															

7 VRF Commands

7.1 address-family

	Use this command to configure an IPv4 address family or IPv6 address family for a multiprotocol VRF.	
	address-family { ipv4 ipv6 }	
Parameter Description	Parameter	Description
	ipv4	Enters IPv4 address family.
	ipv6	Enters IPv6 address family.
Defaults	No IPv4 address family or IPv6 address family is configured for a multiprotocol VRF.	
Command mode	VRF configuration mode	
Usage Guide	This command is applicable only to the multiprotocol VRF.	
Configuration Examples	The following example defines a multiprotocol VRF vrf1 and configures an IPv4 address family. <pre>FS(config)#vrf definition vrf1 FS(config-vrf)#address-family ipv4 FS(config-vrf-af)#</pre>	
Related Commands	Command	Description
	exit-address-family	Exits the VRF address family configuration mode.
	vrf definition	Defines a multiprotocol VRF.
Platform Description	N/A	
	Use this command to configure the VRF description.	
	description string	
Parameter Description	Parameter	Description
	<i>string</i>	VRF description character string. The maximum length is 244 characters.
Defaults	No VRF description is configured by default .	
Command mode	VRF configuration mode	

Usage Guide	N/A						
Configuration Examples	The following example defines a single-protocol IPv4 VRF vrf1 and configure the description to vpn-a. <pre>FS(config)#ip vrf definition vrf1 FS(config-vrf)#description vpn-a</pre> The following example defines a multiprotocol VRF vrf2 and configure the description to vpn-b. <pre>FS(config)#vrf definition vrf1 FS(config-vrf)#description vpn-b</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ip vrf</td><td>Defines a single-protocol IPv4 VRF.</td></tr> <tr> <td>vrf definition</td><td>Defines a multiprotocol VRF.</td></tr> </table>	Command	Description	ip vrf	Defines a single-protocol IPv4 VRF.	vrf definition	Defines a multiprotocol VRF.
Command	Description						
ip vrf	Defines a single-protocol IPv4 VRF.						
vrf definition	Defines a multiprotocol VRF.						
Platform Description	N/A						

7.2 exit-address-family

		Use this command to exit VRF address family configuration mode.
		exit-address-family
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	VRF address family configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example defines a multiprotocol VRF <i>vrf1</i> and configures an IPv4 address family. <pre>FS(config)#vrf definition vrf1 FS(config-vrf)#address-family ipv4 FS(config-vrf-af)# exit-address-family FS(config-vrf)#</pre>	
Related Commands	Command	Description
	address-family	Configures an IPv4 address family or IPv6 address

		family for a multiprotocol VRF.
	vrf definition	Defines a multiprotocol VRF.
Platform Description	N/A	

7.3 ip vrf

	Use this command to create a VRF. Use the no form of this command to delete a VRF.	
	ip vrf <i>vrf-name</i>	
	no ip vrf <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
Defaults	No VRF is configured by default.	
Command mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example creates a VRF. <pre>FS(config)# ip vrf redvrf FS(config-vrf)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.4 ip vrf forwarding

	Use this command to add an interface or sub-interface to a VRF. Use the no form of this command to quit the VRF.	
	ip vrf forwarding <i>vrf-name</i>	
	no ip vrf forwarding <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	Name of the VRF that the interface or sub-interface joins

Defaults	By default, the interface does not belong to any VRF.	
Command mode	Interface configuration mode	
Usage Guide	You can bind the interface to the uni-protocol IPv4 VRF without the IPv6 enabled on the interface. On the device supporting the VRF, if the interface is bound to the uni-protocol IPv4 VRF with the IPv6 protocol enabled, the device cannot forward the IPv6 packets received on this interface.	
Configuration Examples	The following example adds an interface or sub-interface to a VRF. <pre>FS(config-if-GigabitEthernet 0/0)# ip vrf forwarding redvrf</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.5 ip vrf receive

	Use this command to import the host and direct-connected route of one interface into the specified VRF routing table. Use the no form of this command to remove the imported host and direct-connected route from the VRF.	
	ip vrf receive <i>vrf-name</i>	
	no ip vrf receive <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	Name of the VRF that the host and direct-connected route imported to.
Defaults	By default, the host and direct-connected route of the interface are not imported to other VRFs	
Command mode	Interface configuration mode	
Usage Guide	Currently, the ip vrf receive command supports the VRF routing based on the PBR. This command is used to import the host with the main and slave addresses and direct-connected route of this interface into the specified VRF routing table. You need to execute this command multiple times to import this host and direct-connected route to multiple VRF routing tables. Unlike the ip vrf forwarding command, which does not bind the interface to the VRF and this interface still belongs to the global VRF. Configuring both ip vrf forwarding and ip vrf receive on an interface is not allowed. If one has been configured, configuring the other one will prompt an error message. If ip vrf forwarding has been configured, configuring ip vrf receive will prompt: <pre>% Cannot configure 'ip vrf receive' if interface is under a VRF</pre>	

	If ip vrf receive has been configured, configuring ip vrf forwarding will prompt: % Cannot bind interface to a VRF if it has configed 'ip vrf receive'	
Configuration Examples	The following example imports the host and direct-connected route of one interface into the specified VRF routing table. <pre> FS(config)# interface FastEthernet0/1 FS(config-if)# ip address 192.168.1.2 255.255.255.0 FS(config-if)# ip policy route-map PBR-VRF-SELECTION FS(config-if)# ip vrf receive VRF_1 FS(config-if)# ip vrf receive VRF_2 FS(config-if)# end </pre>	
Related Commands	Command	Description
	ip vrf forwarding	Adds the interface to a VRF.
	ip vrf	Creates a VRF.
	set vrf	Sets the VRF in the routing map configuration mode.
Platform Description	N/A	

7.6 maximum routes

	Use this command to set the maximum routes limit within the VRF. Use the no form of this command to remove the setting.	
	maximum routes <i>limit</i> { <i>warn-threshold</i> warning-only }	
	no maximum routes	
Parameter Description	Parameter	Description
	<i>limit</i>	The maximum number of routes, in the range from 1 to 4,294,967,295. The routes which exceed the limits will not be added to the core routing table.
	<i>warn-threshold</i>	The warning will be printed when the threshold is reached. The threshold value is in the range from 1 to 100.
	warning-only	After the number of routes reaches <i>limit</i> , the warning will be printed but the routes will be added to the core routing table.
Defaults	N/A	
Command Mode	Single-protocol VRF is configured in VRF configuration mode; multiple-protocol VRF is configured in address family mode.	
Usage Guide	This command is used to set the maximum number of routes for the VRF.	

Configuration Examples	The following example sets the maximum number of routes for vrf1 to 1,000, and enables the device to only print the warning. <pre>FS(config)# ip vrf vrf1 FS(config-vrf)# maximum routes 1000 warning-only</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.7 vrf definition

	Use this command to create the multiprotocol VRF.	
	vrf definition <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name, no more than 31 characters.
Defaults	N/A	
Command mode	Global configuration mode	
Usage Guide	The single-protocol VRF configuration command ip vrf cannot be used to edit a multiprotocol VRF; the multiprotocol VRF configuration command vrf definition cannot be used to edit a single-protocol IPv4 VRF.	
Configuration Examples	The following example s creates a multiprotocol VRF <i>vrf1</i>. <pre>FS(config)#vrf definition vrf1 FS(config-vrf)#</pre>	
Related Commands	Command	Description
	description	Configures the description.
	address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
	exit-address-family	Exits the VRF address family configuration mode.
	vrf forwarding	Binds a network interface to a multiprotocol VRF.
Platform Description	N/A	

7.8 vrf forwarding

	Use this command to bind a network interface to a multiprotocol VRF.	
	vrf forwarding <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name, which shall be a multiprotocol VRF instead of a single-protocol VRF that supports IPv4 only.
Defaults	The network interface is not bound to any VRF.	
Command mode	Interface configuration mode	
Usage Guide	The configuration command ip vrf forwarding cannot be used to bind a network interface to a multiprotocol VRF; the configuration command vrf forwarding cannot be used to bind a network interface to a single-protocol IPv4 VRF. An interface cannot be bound to a multiprotocol VRF that is not configured with any address family. To bind a network interface to a multiprotocol VRF, you should delete the existing IPv4 addresses, VRRP IPv4 addresses, IPv6 addresses and VRRP IPv6 addresses, and disable IPv6 on the interface. When a network interface is bound to a multiprotocol VRF, no IPv4 address or VRRP IPv4 address should be configured for the interface if no IPv4 address family is configured for the VRF. You should configure an IPv4 address family for the VRF before configuring an IPv4 address and VRRP IPv4 address for the interface. When a network interface is bound to a multiprotocol VRF, no IPv6 address or VRRP IPv6 address should be configured for the interface if no IPv6 address family is configured for the VRF. You should configure an IPv6 address family for the VRF before configuring an IPv6 address and VRRP IPv6 address for the interface. If you delete a multiprotocol VRF's IPv4 address family, you should delete the IPv4 addresses and VRRP IPv4 addresses of all network interfaces bound to the VRF, and delete the IPv4 static routes whose routing VRF or next-hop VRF is that VRF. Likewise, if you delete a multiprotocol VRF's IPv6 address family, you should delete the IPv4 addresses and VRRP IPv6 addresses of all network interfaces bound to the VRF, disable IPv6 on the interfaces, and delete the IPv6 static routes whose routing VRF or next-hop VRF is that VRF.	
Configuration Examples	The following example binds the interface VLAN 1 to a multiprotocol VRF vrf1. <pre> FS(config)#vrf definition vrf1 FS(config-vrf)#address-family ipv4 FS(config-vrf-af)#exit-address-family FS(config-vrf)#address-family ipv6 FS(config-vrf-af)#exit-address-family FS(config-vrf)#interface vlan 1 FS(config-if)#vrf forwarding vrf1 FS(config-if)#ip address 1.1.1.1 255.255.255.0 FS(config-if)#ipv6 address 1000::1/64 </pre>	

Related Commands	Command	Description
	vrf definition	Defines a multiprotocol VRF.
Platform Description	N/A	

7.9 vrf receive

	Use this command to add the local host's route and direct route with the interface's IPv4/v6 address to the routing table of the specified VRF.	
	vrf receive <i>vrf-name</i>	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name, which should be a multiprotocol VRF instead of a single-protocol IPv4 VRF.
Defaults	N/A	
Command mode	Interface configuration mode	
Usage Guide	This command is not used to bind an interface to a VRF, and the interface is still a global interface. If the administrator needs to use PBR to choose VRF, the vrf receive command should be configured on the interfaces where PBR is applied for each selected VRF. When an IPv4 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv4 address is added to the IPv4 routing table of the specified VRF, and the local host's route with the IPv4 address of the master VRRP group on the interface is added to the IPv4 routing table of the specified VRF. When an IPv6 address family is configured for a multiprotocol VRF, the local host's route and direct route with the interface's IPv6 address is added to the IPv6 routing table of the specified VRF, and the local host's route with the IPv6 address of the master VRRP group on the interface is added to the IPv6 routing table of the specified VRF. The ip vrf forwarding and vrf receive commands are mutually exclusive on an interface, and so are the vrf forwarding and vrf receive commands. If both commands are configured on an interface, an error message will be shown. If the ip vrf forwarding or vrf forwarding command is configured first, and then the vrf receive command is configured, the following message will be displayed: <pre>% Cannot configure 'vrf receive' if interface is under a VRF</pre> If the vrf receive command is configured first, and then the ip vrf forwarding or vrf forwarding command is configured, the following message will be displayed: <pre>% Cannot configure 'vrf forwarding vrf2' on this interface, please delete 'ip vrf receive' and 'vrf receive' first.</pre>	
Configuration	The following example selects a VRF using IPv6 PBR on VLAN 1.	

Examples	<pre> FS(config)#vrf definition vrf1 FS(config-vrf)#address-family ipv6 FS(config-vrf-af)#exit-address-family FS(config-vrf)#vrf definition vrf2 FS(config-vrf)#address-family ipv6 FS(config-vrf-af)#exit-address-family FS(config-vrf)#route-map pbr-vrf-selection permit 10 FS(config-route-map)#match ipv6 address acl1 FS(config-route-map)#set vrf vrf1 FS(config-route-map)#route-map pbr-vrf-selection permit 20 FS(config-route-map)#set vrf vrf2 FS(config-route-map)#interface vlan 1 FS(config-if)#ipv6 policy route-map pbr-vrf-selection FS(config-if)#ipv6 address 1000::1/64 FS(config-if)#vrf receive vrf1 FS(config-if)#vrf receive vrf2 </pre>	
Related Commands	Command	Description
	vrf definition	Defines a multiprotocol VRF.
	address-family	Configures an IPv4 address family or IPv6 address family for a multiprotocol VRF.
	set vrf	Configures a VRF in the route map configuration mode.
Platform Description	N/A	

7.10 show ip vrf

	Use this command to display the VRF information.	
	show ip vrf [brief detail interfaces]	
Parameter Description	Parameter	Description
	brief	(Optional) Displays the VRF information in brief.
	detail	(Optional) Displays the VRF information in detail.
	interfaces	(Optional) Displays the VRF's interface information in detail.
Defaults	All VRF information is displayed without parameter specified.	
Command mode	Privileged EXEC mode	
Usage Guide	Use this command to display the VRF information, which can be divided into two levels: Use the keyword brief to display the information in brief. Use the keyword detail to display the information in detail. Use the keyword interfaces to display the VRF's interface information.	
Configuration Examples	The following example displays the VRF information. <pre>FS#show ip vrf Name Interfaces aaa GigabitEthernet 0/0 GigabitEthernet 0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

7.11 show vrf

	Use this command to display the VRF configuration (including the single-protocol VRF and the multiple-protocol VRF).	
	show vrf [ipv4 ipv6 brief count detail]	
Parameter Description	Parameter	Description
	ipv4	Displays the brief VRF (the single-protocol VRF) information of the IPv4 address family.

	IPv6	Displays the VRF brief information of the IPv6 address family.																															
	brief	Displays the brief VRF (including the single-protocol VRF and the multiple-protocol) information.																															
	count	Displays the capacity of VRF and its current value.																															
	detail	Displays the detailed VRF (including the single-protocol VRF and the multiple-protocol) information.																															
Defaults	N/A																																
Command mode	Privileged EXEC mode																																
Usage Guide	N/A																																
Configuration Examples	The following example displays brief information about all VRF. FS#show vrf <table><thead><tr><th>Name</th><th>Default RD</th><th>Protocols</th><th>Interfaces</th></tr></thead><tbody><tr><td>aaa</td><td><not set></td><td>ipv4</td><td></td></tr><tr><td>aab</td><td><not set></td><td></td><td></td></tr><tr><td>bbb</td><td><not set></td><td>ipv6</td><td></td></tr><tr><td>ccc</td><td><not set></td><td>ipv4,ipv6</td><td>VI1</td></tr></tbody></table> : <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Name</td><td>VRF name.</td></tr><tr><td>Default RD</td><td>Default RD of the VRF.</td></tr><tr><td>Protocol</td><td>The address family of the VRF. IPv4 indicates the VRF is enabled in the IPv4 address family mode; ipv6 indicates the VRF is enabled in the IPv6 address family mode.</td></tr><tr><td>Interfaces</td><td>The interface list of the VRF. The interface where the [ip] vrf forwarding command has been configured will be displayed on that list.</td></tr></tbody></table>			Name	Default RD	Protocols	Interfaces	aaa	<not set>	ipv4		aab	<not set>			bbb	<not set>	ipv6		ccc	<not set>	ipv4,ipv6	VI1	Field	Description	Name	VRF name.	Default RD	Default RD of the VRF.	Protocol	The address family of the VRF. IPv4 indicates the VRF is enabled in the IPv4 address family mode; ipv6 indicates the VRF is enabled in the IPv6 address family mode.	Interfaces	The interface list of the VRF. The interface where the [ip] vrf forwarding command has been configured will be displayed on that list.
Name	Default RD	Protocols	Interfaces																														
aaa	<not set>	ipv4																															
aab	<not set>																																
bbb	<not set>	ipv6																															
ccc	<not set>	ipv4,ipv6	VI1																														
Field	Description																																
Name	VRF name.																																
Default RD	Default RD of the VRF.																																
Protocol	The address family of the VRF. IPv4 indicates the VRF is enabled in the IPv4 address family mode; ipv6 indicates the VRF is enabled in the IPv6 address family mode.																																
Interfaces	The interface list of the VRF. The interface where the [ip] vrf forwarding command has been configured will be displayed on that list.																																
Related Commands	Command	Description																															
	N/A	N/A																															
Platform Description	N/A																																

8 RIPng Commands

8.1 clear ipv6 rip

	Use this command to clear the RIPng routes.	
	clear ipv6 rip	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	None	
Command mode	Privileged EXEC mode	
Usage Guide	Running this command removes all RIPng routes and this operation may have great impact on the RIPng protocol. This command should be used with caution.	
Configuration Examples	The following example clears the RIPng routes: FS# clear ipv6 rip	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.2 default-metric

	Use this command to configure the default metric for RIPng. Use the no form of this command to restore the default value.	
	default-metric <i>metric</i>	
	no default-metric	
Parameter Description	Parameter	Description
	<i>metric</i>	Sets the default metric value. The valid range is from 1 to 16. The route is unreachable if the metric value is larger than or equal to 16.
Defaults	The default value is 1.	

Command mode	Routing process configuration mode.	
Usage Guide	This command shall be used with the redistribute command. When redistributing the route from one route process to RIPvng, due to the incompatibility of metric calculation mechanisms of different routing protocols, it fails to translate the routing metric values. To this end, the RIPvng metric value shall be defined when translating the metric values. If there is no defined metric value, use the default-metric command to define one; and the defined metric value will overwrite the value of the default-metric command. By default, the default-metric value is 1.	
Configuration Examples	The following example shows how to set the RIPvng metric value as 3 when redistributing OSPF process 100: FS(config-router)# default-metric 3 FS(config-router)# redistribute ospf 100	
Related Commands	Command	Description
	redistribute	Redistributes the route from one route domain to another route domain.
Platform Description	N/A	

8.3 distance

	Use this command to set the administrative distance of RIPv6. Use the no form of this command to restore the default value.	
	distance <i>distance</i>	
	no distance	
Parameter Description	Parameter	Description
	<i>distance</i>	Sets the RIPv6 administrative distance. The range is from 1 to 254.
Defaults	The default distance is 120	
Command mode	Routing process configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example shows how to set the RIPv6 administrative distance as 160: FS(config)# ipv6 router rip FS(config-router)# distance 160	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.4 distribute-list

	Use this command to filter the in/out route in the prefix list. Use the no form of this command to remove route filtering.	
	distribute-list prefix-list <i>prefix-list-name</i> { in out } [<i>interface-type interface-name</i>]	
	no distribute-list prefix-list <i>prefix-list-name</i> { in out } [<i>interface-type interface-name</i>]	
Parameter Description	Parameter	Description
	prefix-list <i>prefix-list-name</i>	Name of the prefix list which is used to filter the route.
	in out	Filters the in or out route in the distribute list.
	<i>interface-type interface-name</i>	(Optional) Applies the distribute list to the specified interface.
Defaults	By default, no distribute list is defined.	
Command mode	Routing process configuration mode.	
Usage Guide	This command is used to configure the route distribution control list to filter all update routes for the purpose of refusing to receive or send the specified routes. If the interface is not specified, the update routes on all interfaces are filtered.	
Configuration Examples	The following example shows how to filter the received update route on the interface eth0 (only those update routes within the prefix-list allowpre prefix list range can be received) <pre>FS(config)# ipv6 router rip FS(config-router)# distribute-list prefix-list allowpre in eth0</pre>	
Related Commands	Command	Description
	redistribute	Sets route redistribution.
Platform Description	N/A	

8.5 graceful-restart

	Use this command to configure the graceful restart (GR) function for the RIPng process. graceful-restart [grace-period <i>grace-period</i>]

	Use the no form of this command restore the default configurations. no graceful-restart [grace-period]	
Parameter Description	Parameter	Description
	graceful-restart	Enables the GR function.
	grace-period	Displays the configured grace period.
	<i>grace-period</i>	Indicates the configured GR period, ranging from 1 to 1800 seconds. The default value is the smaller between twice of the update time and 60s.
Defaults	The GR function is enabled by default.	
Command Mode	Routing process configuration mode	
Default Level	14	
Usage Guide	The GR function is configured based on RIPv6 instances. Different parameters can be configured for different RIPv6 instances as required. The GR period indicates the maximum duration from RIPv6 restart to RIPv6 GR completion. In this time period, the forwarding table before restart is used and the RIPv6 route is restored to the status before restart. After the GR period expires, the RIPv6 process exits the GR status and the common RIPv6 operation is performed. The graceful-restart grace-period command allows a user to modify the GR period in explicit mode. Note that GR is completed and the RIPv6 route is updated once before the RIPv6 route becomes invalid. If the GR period is improperly set, continuous data forwarding in the GR process cannot be ensured. A typical case is as follows: If the GR period is greater than the invalid time of the neighbor route, GR is not completed before the route becomes invalid and the route is not advertised to the neighbor again. The neighbor route stops forwarding data after the route becomes invalid, resulting in data forwarding interruption. Therefore, unless otherwise specified, it is not recommended to adjust the GR period. If the GR period needs to be configured, check configuration of the timers command to ensure that the GR period value is greater than the route update time and smaller than the route invalid time. When GR is performed for the RIPv6 process, ensure that the network environment is stable.	
Configuration Examples	The following example enables the GR function for the RIPv6 process and configures the GR period. <pre>FS(config)# ipv6 router rip FS(config-router)# graceful-restart grace-period 90</pre>	
Verification	Run the show ipv6 rip command to check whether the GR function is configured and query the configured grace period.	
Prompts	N/A	
Common Errors	N/A	
Platform	N/A	

Description	

8.6 ipv6 rip default-information

	Use this command to generate a default IPv6 route to the RIPv6. Use the no form of this command to remove the default route.	
	ipv6 rip default-information { only originate } [metric <i>metric-value</i>]	
	no ipv6 rip default-information	
Parameter Description	Parameter	Description
	only	Advertises the IPv6 default route only.
	originate	Advertises both of the IPv6 default route and other routes.
	metric <i>metric-value</i>	Sets the metric value for the default route. The valid range is from 1 to 15. The default metric is 1.
Defaults	By default, no default route is configured.	
Command mode	Interface configuration mode	
Usage Guide	With this command configured on an interface, the interface advertises an IPv6 default route and the route itself is not to join the device route forwarding table and the RIPv6 route database. To avoid the route loop, once this command has been configured on the interface, RIPv6 refuses to receive the default route update message advertised from the neighbor.	
Configuration Examples	The following example shows how to create a default route to the RIPv6 routing process on the interface ethernet0/0 and enable this interface to advertise the default route only: <pre>FS(config)# interface ethernet 0/0 FS(config-if)# ipv6 rip default-information only</pre>	
Related Commands	Command	Description
	show ipv6 rip	Displays the RIPv6 process and statistics.
	show ipv6 rip database	Displays the RIPv6 route.
Platform Description	N/A	

8.7 ipv6 rip enable

	Use this command to enable the RIPv6 on the interface. Use the no form of this command to disable RIPv6 on the interface.
	ipv6 rip enable
	no ipv6 rip enable

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	It is disabled by default.	
Command mode	Interface configuration mode.	
Usage Guide	This command is used to add the RIPng interface. Before this command is configured, if the RIPng is not enabled, use this command to enable the RIPng automatically.	
Configuration Examples	The following example shows how to enable the RIPng on the interface 0/0: <pre>FS(config)# interface ethernet 0/0 FS(config-if)# ipv6 rip enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.8 ipv6 rip metric-offset

	Use this command to set the interface metric value. Use the no form of this command to remove the metric configurations.	
	ipv6 rip metric-offset <i>value</i>	
	no ipv6 rip metric-offset	
Parameter Description	Parameter	Description
	<i>value</i>	Sets the interface metric value on the interface. The valid range is from 1 to 16.
Defaults	The default value is 1.	
Command mode	Interface configuration mode.	
Usage Guide	Before the route is added to the routing list, the interface metric value shall be upon the route metric. To this end, the interface metric value influences the route usage.	

Configuration Examples	The following example shows how to set the metric value of the interface Ethernet 0/1 as 5:	
	<pre>FS(config)# interface ethernet 0/1 FS(config-if)# ipv6 rip metric-offset 5</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.9 ipv6 rip subvlan

	Use this command to enable RIPng on super VLANs. Use the no form of this command to restore the default setting. <pre>ipv6 rip subvlan [all vid] no ipv6 rip subvlan</pre>	
Parameter Description	Parameter	Description
	all	Indicates that packets are allowed to be sent to all sub VLANs.
	vid	Specifies the sub VLAN ID. The value ranges from 1 to 4094.
Defaults	The default setting takes effect only on super VLANs with RIPng disabled.	
Command Mode	Interface configuration mode.	
Usage Guide	In normal cases, a super VLAN contains multiple sub VLANs. Multicast packets of a super VLAN are also sent to its sub VLANs. In this case, when RIPng multicast packets are sent over a super VLAN containing multiple sub VLANs, the RIPng multicast packets are replicated multiple times, and the device processing capability is insufficient. As a result, a large number of packets are discarded, causing the neighbor down error. In most scenarios, the RIPng function does not need to be enabled on a super VLAN. Therefore, the RIPng function is disabled by default. However, in some scenarios, the RIPng function must be run on the super VLAN, but packets only need to be sent to one sub VLAN. In this case, run this command to specify a particular sub VLAN. You must be cautious in configuring packet transmission to all sub VLANs, as the large number of sub VLANs may cause a device processing bottleneck, which will lead to the neighbor down error.	
Configuration	The following example sends the RIPng multicast packets to sub VLAN 1024 of super VLAN 300.	

Examples	FS(config)# interface vlan 300
	FS(config-if-VLAN 300)# ipv6 rip subvlan 1024

8.10 ipv6 router rip

	Use this command to create the RIPng process and enter routing process configuration mode. Use the no form of this command to remove the RIPng process.	
	ipv6 router rip	
	no ipv6 router rip	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	No RIPng process is configured by default.	
Command mode	Global configuration mode.	
Usage Guide	N/A.	
Configuration Examples	The following example shows how to create the RIPng process and enter routing process configuration mode: FS(config)# ipv6 router rip	
Related Commands	Command	Description
	ipv6 rip enable	Enables the RIPng on the specified interface.
Platform Description	N/A	

8.11 passive-interface

	Use this command to disable the interface to send update packets. Use the no form of this command to enable the interface to send update packets.	
	passive-interface { default interface-type interface-num }	
	no passive-interface { default interface-type interface-num }	
Parameter Description	Parameter	Description
	default	Enables the passive mode on all interfaces.
	<i>interface-type interface-num</i>	Interface type and interface number.
Defaults	No passive interface is configured by default.	

Command mode	Routing process configuration mode.	
Usage Guide	You can use the passive-interface default command to enable the passive mode on all interfaces. Then ,use the no passive-interface interface-type interface-num command to remove the specified interface from the passive mode.	
Configuration Examples	The following example shows how to enable the passive mode on all interfaces and remove interface ethernet 0/0 from the passive mode: <pre>FS(config-router)# passive-interface default FS(config-router)# no passive-interface ethernet 0/0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.12 redistribute

	Use this command to redistribute the route of other routing protocols to RIPng. Use the no form of this command to remove the redistribution configuration.	
	redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> static } [metric <i>metric-value</i> route-map <i>route-map-name</i>]	
	no redistribute { bgp connected isis [<i>area-tag</i>] ospf <i>process-id</i> static } [metric <i>metric-value</i> route-map <i>route-map-name</i>]	
Parameter Description	Parameter	Description
	bgp	Redistributes the BGP routes to RIPng.
	connected	Redistributes the connected routes to RIPng.
	isis [<i>area-tag</i>]	Redistributes the ISIS routes to RIPng. <i>area-tag</i> indicates the ISIS process number.
	ospf <i>process-id</i>	Redistributes the OSPF routes to RIPng. <i>process-id</i> indicates the OSPF process number, and the range is from 1 to 65,535.
	static	Redistributes the static routes to RIPng.
	metric <i>metric-value</i>	(Optional) Sets the metric value for the route redistributed to RIPng.
	route-map <i>route-map-name</i>	(Optional) Sets the redistribution route filtering.
Defaults	By default, the routes of other routing protocols are not redistributed. If the default-metric command is not configured, the default metric value is 1;	

	By default, the route-map is not configured; By default, all sub-type routes in the specified routing process are redistributed.	
Command mode	Routing process configuration mode.	
Usage Guide	This command is used to redistribute the external routes to RIPng. It is unnecessary to transform the metric of one routing protocol into another routing protocol in the process of the route redistribution, for the metric calculation methods of the different routing protocols are different. The RIP and OSPF metric calculations are incomparable for the reason that the RIP metric calculation is hop-based while the OSPF one is bandwidth-based. The instance, from where the routing information is redistributed to the RIPng, must be specified in the process of configuring the multi-instance protocol redistribution.	
Configuration Examples	The following example shows how to redistribute the static route, use the route map <i>mymap</i> to filter and set the metric value as 8: <pre>FS(config)# ipv6 router rip FS(config-router)# redistribute static route-map mymap metric 8</pre>	
Related Commands	Command	Description
	default-metric	Defines the default RIPng metric value when redistributing other routing protocols.
	distribute-list	Filters the RIPng routing update packets.
Platform Description	N/A	

8.13 show ipv6 rip

	Use this command to show the parameters and each statistical information of the RIPng routing protocol process.	
	show ipv6 rip	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode or user mode.	
Usage Guide	N/A	

Configuration	FS# show ipv6 rip										
Examples	Routing Protocol is "RIPng" Sending updates every 10 seconds with +/-50%, next due in 8 seconds Timeout after 30 seconds, garbage collect after 60 seconds Outgoing update filter list for all interface is: distribute-list prefix aa out Incoming update filter list for all interface is: not set Default redistribution metric is 1 Default distance is 120 Redistribution: Redistributing protocol connected route-map rm Redistributing protocol static Redistributing protocol ospf 1 Default version control: send version 1, receive version 1 <table> <tr> <td>Interface</td><td>Send</td><td>Recv</td></tr> <tr> <td>VLAN 1</td><td>1</td><td>1</td></tr> <tr> <td>Loopback 1</td><td>1</td><td>1</td></tr> </table> Routing Information Sources: None		Interface	Send	Recv	VLAN 1	1	1	Loopback 1	1	1
Interface	Send	Recv									
VLAN 1	1	1									
Loopback 1	1	1									
Related Commands	Command	Description									
	show ipv6 rip	Displays the parameters and each statistical information of the RIPng process.									
Platform Description	N/A										

8.14 show ipv6 rip database

	Use this command to display the RIPng route entries.	
	show ipv6 rip database	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command mode	Privileged EXEC mode or user mode.	
Usage Guide	N/A	

Configuration	FS# show ipv6 rip database	
Examples	Codes: R - RIPv6, C - Connected, S - Static, O - OSPF, B - BGP sub-codes: n - normal, s - static, d - default, r - redistribute, i - interface, a/s - aggregated/suppressed S(r) 2001:db8:1::/64, metric 1, tag 0 Loopback 0/:: S(r) 2001:db8:2::/64, metric 1, tag 0 Loopback 0/:: C(r) 2001:db8:3::/64, metric 1, tag 0 VLAN 1/:: S(r) 2001:db8:4::/64, metric 1, tag 0 Null 0/:: C(i) 2001:db8:5::/64, metric 1, tag 0 Loopback 1/:: S(r) 2001:db8:6::/64, metric 1, tag 0 Null 0/::	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.15 split-horizon

	Use the split-horizon command to enable the RIPv6 split-horizon function in routing process configuration mode. Use the no form of this command to disable this function. Use the split-horizon poisoned-reverse command to enable the RIPv6 poisoned reverse horizontal split function in routing process configuration mode. Use the no form of this command to disable this function.	
	split-horizon [poisoned-reverse]	
	no split-horizon [poisoned-reverse]	
Parameter Description	Parameter	Description
	poisoned-reverse	(Optional) Enables the poisoned-reverse horizontal split.
Defaults	RIPv6 split horizon is enabled by default.	
Command mode	Routing process configuration mode.	
Usage Guide	In the process of packet updating, split-horizon function prevents some routing information from being	

	advertised through the interface learning those routing information. The poisoned reverse horizontal split function advertises some routing information to the interface learning those routing information, and the metric value is set as 16. The RIPng routing protocol belongs to the distance vector routing protocol, so the horizontal split shall be noticed in the actual application. You can use the show ipv6 rip command to determine whether the RIPng split-horizon function is enabled or not.	
Configuration Examples	The following example shows how to disable the RIPng horizontal split: <pre>FS(config)# ipv6 router rip FS(config-router)# no split-horizon</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.16 timers

	Use this command to adjust the RIPng timer. Use the no form of this command to restore the default settings.	
	timers update invalid flush	
	no timers	
Parameter Description	Parameter	Description
	<i>update</i>	Sets the routing update time, in seconds. The update parameter defines the period of sending the routing update packets by the device. The invalid and flush parameter reset once the update packets are received.
	<i>invalid</i>	Sets the routing invalid time, in seconds, starting from receiving the last valid update packet. The invalid parameter defines the invalid time for the un-updated routing in the routing list. The routing invalid time shall be three times larger than the routing update time. The routing will be invalid if no update packets are received within the routing invalid time, and it will reset if the update packets are received within the invalid time.
	<i>flush</i>	Sets the routing flush time, in seconds, starting from RIPng entering to invalid state. The invalid routing will be removed from the routing list if the flush time expires.
Defaults	The default update time is 30 seconds; the default invalid time is 180 seconds; and the default flush time is 120 seconds.	
Command mode	Routing process configuration mode.	

Usage Guide	Adjusting the above time may speed up the RIPv6 convergence time and the troubleshooting time. The RIPv6 time must be consistent for the devices connecting to the same network. You are not recommended to adjust the RIPv6 time, except for the specific requirement. Use the show ipv6 rip command to view the current RIPv6 time parameter setting. In the low-speed link, with the short time configured, large amount of the update packets consumes a lot of bandwidth. Generally, the short time can be configured in the Ethernet or 2Mbps-higher line to shorten the convergence time of the network routing.	
Configuration Examples	The following example shows how to send the RIPv6 update packets every 10 seconds. The routing will be invalid if no update packets are received within 30 seconds, and the routing will be removed after being invalid for 90 seconds. <pre>FS(config)# ipv6 router rip FS(config-router)# timers 10 30 90</pre>	
Related Commands	Command	Description
	show ipv6 rip	Displays the parameters and the statistical information of the RIPv6 process.
	show ipv6 rip database	Displays the RIPv6 routes.
Platform Description	N/A	

9 NSM Commands

9.1 clear ip route

	Use this command to clear the route cache.	
	clear ip route [vrf <i>vrf_name</i>] { * <i>network</i> [<i>netmask</i>] }	
Parameter Description	Parameter	Description
	vrf <i>vrf_name</i>	(Optional) Specifies the route cache of the specified VRF instance. If no VRF is specified, the route cache of all VRF instances is cleared.
	*	Clears all route cache.
	network	Specifies the route cache of the network or subnet.
	netmask	(Optional) Subnet mask. If no subnet mask is specified, the longest match principle is used when you match <i>network</i> with the route. The cache of the longest match is cleared.
Command Mode	Privileged EXEC mode	
Usage Guide	Clearing route cache clears the corresponding routes and triggers the routing protocol relearning. Please note that clearing all route cache leads to temporary network disconnection.	
Examples	The following example clears the cache of the route which is the longest match with IP address 192.168.12.0. clear ip route 192.168.12.0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	This command is not supported on 2-layer devices.	

9.2 ip default-network

	Use this command to configure the default network globally. Use the no or default form of this command to restore the default setting.	
	ip default-network <i>network</i> no ip default-network <i>network</i> default ip default-network <i>network</i>	
Parameter Description	Parameter	Description
	<i>network</i>	Default network
Defaults	The default is 0.0.0.0/0.	
Command Mode	Global configuration mode	
Usage Guide	The goal of this command is to generate the default route. The default network must be reachable in the routing table, but not the directly connected network. The default network always starts with an asterisk ("*"), indicating that it is the candidate of the default route. If there is connected route and the route without the next hop in the default network, the default route must be a	

	static route.	
Examples	The following example sets 192.168.100.0 as the default network. Since the static route to the network is configured, the device will automatically generate a default route.	
	<pre>ip route 192.168.100.0 255.255.255.0 serial 0/1</pre>	
	<pre>ip default-network 192.168.100.0</pre>	
	The following example sets 200.200.200.0 as the default network. The route becomes the default one only when it is available in the routing table.	
Related Commands	<pre>ip default-network 200.200.200.0</pre>	
Related	Command	Description
Commands	show ip route	Displays the routing table.

9.3 ip fast-reroute route-map

	Use this command to enable static fast reroute. Use the no or default form of this command to restore the default setting.	
	ip fast-reroute [vrf <i>vrf-name</i>] static route-map <i>route-map-name</i>	
	no ip fast-reroute [vrf <i>vrf-name</i>]	
	default ip fast-reroute [vrf <i>vrf-name</i>] route-map	
Parameter	Parameter	Description
Description	vrf <i>vrf-name</i>	VRF
	route-map <i>route-map-name</i>	Route map
	static	Backup route
Default	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage guideline	Fast reroute provides an active next-hop and a backup one. If the active next-hop fails, the backup next-hop is used for forwarding. To enhance the performance of fast reroute, enable the BFD detection function for the active next-hop. For interfaces that are up or down, to shorten the interruption time of fast reroute, configure carrier-delay 0 in the <i>interface configuration mode of the active outbound interface to optimize the performance</i>. For static fast reroute, if the active next-hop fails, the backup next-hop is used for forwarding.	
Examples	The following example sets the backup next-hop of all static routes to 192.168.1.2 through the outbound interface of GigabitEthernet 0/1. <pre>FS(config)# route-map fast-reroute FS(config-route-map)# set fast-reroute backup-nexthop GigabitEthernet 0/1 192.168.1.2 FS(config-route-map)# exit FS(config)# ip fast-reroute static route-map fast-reroute</pre>	

Related command	Command	Description
	fast-reroute	Configures OSPF fast reroute.
Platform Description	This command is not supported on 2-layer devices.	

9.4 ip route

	Use this command to configure a static route. Use the no or default form of this command to restore the default setting.	
	ip route [vrf <i>vrf_name</i>] <i>network net-mask</i> { <i>ip-address</i> <i>interface</i> [<i>ip-address</i>] } [<i>distance</i>] [tag <i>tag</i>] [permanent { track <i>object-number</i> arp }] [weight <i>number</i>] [description <i>description-text</i>] [disabled enabled] [global]	
	no ip route [vrf <i>vrf_name</i>] <i>network net-mask</i> { <i>ip-address</i> <i>interface</i> [<i>ip-address</i>] } [<i>distance</i>]	
	no ip route [vrf <i>vrf_name</i>] all	
	default ip route [vrf <i>vrf_name</i>] <i>network net-mask</i> { <i>ip-address</i> <i>interface</i> [<i>ip-address</i>] } [<i>distance</i>]	
	default ip route [vrf <i>vrf_name</i>] all	
Parameter Description	Parameter	Description
	vrf <i>vrf_name</i>	Name of the VRF, which can be the single protocol IPv4 VRF or configured IPv4 address family multi-protocol VRF.
	<i>network</i>	Network address of the destination
	<i>net-mask</i>	Mask of the destination
	<i>ip-address</i>	The next hop IP address of the static route
	<i>interface</i>	(Optional) The next hop egress of the static route
	<i>distance</i>	(Optional) The administrative distance of the static route
	<i>tag</i>	(Optional) The tag of the static route
	permanent	(Optional) Permanent route ID
	track <i>object-number</i>	(Optional) Indicates correlation with Track. <i>object-number</i> indicates the ID of the track object. By default, the static route is not correlated with the Track function.
	weight <i>number</i>	(Optional) Indicates the weight of the static route. The weight is 1 by default.
	description <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.
	disabled/enabled	(Optional) Indicates the enable flag of the static route. The flag is enabled by default.
	global	(Optional) Indicates that the next hop belongs to a global VRF. By default, the VRF of the next hop is the same as the VRF specified by <i>vrf name</i> .
Defaults	No static route is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route	

	backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails. You can specify the VRF that the static route belongs to. The default weight of the static route is 1. To view the static route of non default weight, execute the show ip route weight command. The parameter weight is used to enable WCMP. When there are load-balanced routes to the destination, the device assigns data flows by their weights. The higher the weight of a route is, the more data flow the route carries. WCMP limit is generally 32 for routers. However, WCMP limit varies by switch models for their chipsets support different weights. When the sum of the weights of load balanced routes is beyond this weight limit, the excessive ones will not take effect. Enablement/disablement shows the state of the static route. Disablement means the static route is not used for forwarding. The forwarding table used the permanent route until administrator deletes it. Association between a static route and an ARP object can be specified. When association between a static route and an ARP object is configured and the ARP object corresponding to the next hop and egress of the route does not exist, the static route does not take effect. When the ARP object corresponding to the next hop and egress of the route exists, the static route takes effect based on another status. Association between a static route and an ARP object cannot be used for routes with the permanent attribute.
Examples	The following example adds a static route to the destination network of 172.16.100.0/24 whose next hop is 192.168.12.1 and administrative distance is 15. <pre>ip route 172.16.199.0 255.255.255.0 192.168.12.1 155</pre> If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures data flows to be sent through fastethernet 0/0 to the destination network of 172.16.100.0/24. <pre>ip route 172.16.199.0 255.255.255.0 fastethernet 0/0 192.168.12.1</pre>
Related Commands	This command is not supported on 2-layer devices.

9.5 ip route static bfd

	Use this command to correlate the static route with BFD. Use the no or default form of this command to restore the default setting.	
	ip route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
	no ip route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
	default ip route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
	Use this command to correlate the static route with BFD. Use the no or default form of this command to restore the default setting.	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
	<i>interface-type interface-number</i>	Interface type and interface number.
	<i>gateway</i>	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
	source <i>ip-address</i>	(Optional) The source IP address of the BFD session. If the

		neighbor device is multi hops away, you should specify the source IP address for the BFD session. No source IP address is specified by default.
Defaults	The static address is not correlated with BFD by default.	
Command Mode	Global configuration mode	
Usage Guide	 Please make sure the BFD session parameters have been configured before executing this command.	
Examples	The following example correlates the static route with BFD, and detects the reachability of path to the neighbor 172.16.0.2. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# no switchport // No need to perform this command on the router. FS(config-if-GigabitEthernet 0/1)# ip address 172.16.0.1 255.255.255.0 FS(config-if-GigabitEthernet 0/1)# bfd interval 50 min_rx 50 multiplier 3 FS(config-if-GigabitEthernet 0/1)# exit FS(config)# ip route static bfd GigabitEthernet 0/1 172.16.0.2 FS(config)# ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/1 172.16.0.2</pre>	
Related Commands	N/A	
Platform Description	This command is not supported on 2-layer devices.	

9.6 ip route static inter-vrf

	Use this command to enable packets to be forwarded over VRF instances through the static route. Use the no or default form of this command to disable this function.	
	ip route static inter-vrf	
	no ip route static inter-vrf	
	default ip route static inter-vrf	
	Use this command to enable packets to be forwarded over VRF instances through the static route. Use the no or default form of this command to disable this function.	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	If the no form of this command is executed, packets are unable to be forwarded over VRF instances through the static route. If this command is executed and you want to use the no form of this command to disable such function, the following information will be displayed. <pre>*Aug 7 10:58:34: %NSM-6-ROUTESACROSSVRF: Un-installing route [x.x.x.x/8] from global routing table with outgoing interface x/x.</pre>	
Examples	The following example disables packets to be forwarded over VRF instances through the static route. <pre>FS(config)# no ip route static inter-vrf</pre>	
Related	N/A	

Commands	
Platform	
Description	This command is not supported on 2-layer devices.

9.7 ip routing

	Use this command to enable IP routing in the global configuration mode. Use the no or default form of this command to disable this function. ip routing no ip routing default ip routing
Defaults	This function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	IP routing is not necessary when the switch serves as bridge or VoIP gateway. When a device functions only as a bridge or VoIP gateway, the IP routing function of the FSOS software is not required. In this case, the IP routing function of the FSOS software can be disabled. After the IP routing function is disabled, the device functions as a common host. The device can send and receive packets but cannot forward packets. All route-related configurations will be deleted except the static route configuration. A large number of static routes may be configured. If a user runs the no ip routing command, the configuration of a large number of static routes may be lost. To prevent this situation, the static route configuration will be hidden temporarily when the no ip routing command is run. If the ip routing command is run again, the static route configuration can be restored. Note that if the process or whole system restarts when the no ip routing command is run, the static route configuration will not be reserved.
Examples	The following example disables IP routing. <pre>FS(config)# no ip routing</pre>
Related Commands	N/A
Platform	
Description	This command is not supported on 2-layer devices.

9.8 ip static route-limit

	Use this command to set the upper threshold of the static route. Use the no or default form of this command to restore the default setting.	
	ip static route-limit <i>number</i>	
	no ip static route-limit	
	default ip static route-limit	
Parameter	Parameter	Description
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000
Defaults	The default is 1000.	
Command Mode	Global configuration mode	
Usage Guide	The goal is to control the number of static routes. You can view the upper threshold of the configured non-default	

	static routes with the show running-config command.
Examples	The following example sets the upper threshold of the static routes to 9000 and then restores the setting to the default value. <pre>FS(config)#ip static route-limit ? <1-1000000> Global limit value(default value: 1000) FS(config)# ip static route-limit 9000 FS(config)# no ip static route-limit</pre>
Related Commands	N/A
Platform	
Description	This command is not supported on 2-layer devices.

9.9 ipv6 route

	Use this command to configure an ipv6 static route. Use the no or default form of this command to restore the default setting.	
	ipv6 route [vrf <i>vrf-name</i>] <i>ipv6-prefix / prefix-length</i> { <i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }] <i>interface</i> [<i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }]] } [<i>distance</i>] [tag <i>tag</i>] [weight <i>number</i>] [description <i>description-text</i>]	
	no ipv6 route [vrf <i>vrf-name</i>] <i>ipv6-prefix / prefix-length</i> { <i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }] <i>interface</i> [<i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }]] } [<i>distance</i>]	
	no ipv6 route [vrf <i>vrf_name</i>] all	
	default ipv6 route [vrf <i>vrf-name</i>] <i>ipv6-prefix / prefix-length</i> { <i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }] <i>interface</i> [<i>ipv6-address</i> [nexthop-vrf { <i>vrf-name1</i> default }]] } [<i>distance</i>]	
	default ipv6 route [vrf <i>vrf_name</i>] all	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	Name of VRF, which must be the configured IPv6 address family multi-protocol VRF
	<i>prefix-length</i>	Mask length of the destination
	<i>ipv6-address</i>	The next hop IP address of the static route
	<i>interface</i>	(Optional) The next hop egress of the static route
	nexthop-vrf <i>vrf-name1</i>	(Optional) VRF the nexthop belongs, which must be the configured IPv6 address family multi-protocol VRF.
	<i>distance</i>	(Optional) The administrative distance of the static route. The default is 1.
	<i>tag</i>	(Optional) The tag value of the static route. The default is 0.
	weight <i>number</i>	(Optional) Indicates the weight of the static route, which must be specified when you configure equal-cost routes. The weight ranges from 1 to 8. When the weights of all equal-cost routes of a route are summed up, the sum cannot exceed the maximum number of equal-cost routes that can be configured for the route. Weighting of equal-cost routes of a route indicates the traffic ratio

		of these routes. The weight is 1 by default.
	description <i>description-text</i>	(Optional) Indicates the description of the static route. By default, no description is configured. <i>description-text</i> is a string of one to 60 characters.
Defaults	No IPv6 static route is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	When the multi-protocol VRF deletes the IPv6 address family, the IPv6 static route of VRF that the route or nexthop belongs is deleted. If the VRF of the IPv6 static route interface is not same as the nexthop's VRF, then this IPv6 static route takes no effect. The default administrative distance of the static route is 1. Setting the administrative distance allows the learnt dynamic route to overwrite the static route. Setting the administrative distance of the static route can enable route backup, which is called floating route in this case. For example, the administrative distance of the OSPF is 110. You can set its administrative distance to 125. Then the data can switch over the static route when the route running OSPF fails.	
Examples	The following example adds a static route to the destination network of 2001::/64 whose next hop is 2002::2 and administrative distance are 115. <pre>ipv6 route 2001::/64 2002::2 115</pre> If the static route has not a specific interface, data flows may be sent through other interface in case of interface failure. The following example configures that data flows are sent through fastethernet 0/0 to the destination network of 2001::/64. <pre>ipv6 route 2001::/64 fastethernet 0/0 2002::2</pre>	
Related Commands	Command	Description
	show ipv6 route	Displays IPv6 routing table.
Platform Description	This command is not supported on 2-layer devices.	

9.10 ipv6 route static bfd

	Use this command to correlate the static route with BFD. Use the no or default form of this command to restore the default setting.	
	ipv6 route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
	no ipv6 route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
	default ipv6 route static bfd [vrf <i>vrf-name</i>] <i>interface-type interface-number gateway</i> [source <i>ip-address</i>]	
Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	(Optional) Specifies the VRF name of the static route. By default, it is global VRF,
	<i>interface-type interface-number</i>	Interface type and interface number.
	<i>gateway</i>	Specifies the gateway IP address, that is, the BFD neighbor IP address. If the next hop of the static route is the neighbor, the BFD will detect whether this neighbor is reachable.
	source <i>ipv6-address</i>	(Optional) The source IP address of the BFD session. If the neighbor device is multi hops away, you should specify the source

		IP address for the BFD session. No source IP address is specified by default.
Defaults	The static route is not associated with BFD by default.	
Command Mode	Global configuration mode	
Usage Guide	 Please make sure the BFD session parameters have been configured before executing this command.	
Examples	The following example correlates the static route with BFD, and detects the reachability of path to the neighbor 2001:1::2. <pre>FS(config)# interface GigabitEthernet 0/1 FS(config-if)# no switchport // FS(config-if)# ip address 2001:1::1/64 FS(config-if)# bfd interval 50 min_rx 50 multiplier 3 FS(config-if)# exit FS(config)# ipv6 route static bfd GigabitEthernet 0/1 2001:1::2 FS(config)# ipv6 route 2002::/64 GigabitEthernet 0/1 2001:1::2</pre>	
Related Commands	N/A	
Platform		
Description	This command is not supported on 2-layer devices.	

9.11 ipv6 static route-limit

	Use this command to set the upper threshold of the static route. Use the no or default form of this command to restore the default setting.
	ipv6 static route-limit <i>number</i>
	no ipv6 static route-limit
	default ipv6 static route-limit

Parameter	Parameter	Description
Description	<i>number</i>	Upper threshold of static routes in the range from 1 to 10000.

Defaults	The default is 1000.

Command Mode	Global configuration mode

Usage Guide	The goal is to control the number of static routes. You can view the upper threshold of the configured non-default static routes with the show running config command.

Examples	The following example sets the upper threshold of global ipv6 static routes to 900, default VRF static routes to 200, VRF test static routes to 100, and then restores the setting to the default value. <pre>FS(config)#ipv6 static route-limit ? <1-10000> Global limit value(default value: 1000)</pre>

	FS(config)# ipv6 static route-limit 900 FS(config)# no ipv6 static route-limit

Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.
	show ipv6 route	Displays the IPv6 routing table.

Platform Description	This command is not supported on 2-layer devices.

9.12 ipv6 unicast-routing

	Use this command to enable the IPv6 route function of the FSOS. Use the no or default form of this command to disable this function.
	ipv6 unicast-routing
	no ipv6 unicast-routing
	default ipv6 unicast-routing

Parameter Description	N/A

Defaults	This function is enabled by default.

Command Mode	Global configuration mode

Usage Guide	This function can be disabled if the device is just used as the bridge-connection device or the VOIP gateway device.

Examples	The example disables the IPv6 route function of FSOS. FS# no ipv6 unicast-routing

Related Commands	Command	Description
	ipv6 route	Configure the IPv6 static route.
	show ipv6 route	Displays the IPv6 routing table.

Platform Description	This command is not supported on 2-layer devices.

9.13 maximum-paths

	Use this command to specify the number of equivalent routes. Use the no or default form of this command is used to restore the default setting.
	maximum-paths <i>number</i>
	no maximum-paths
	default maximum-paths

Parameter	Parameter	Description
Description	<i>number</i>	Number of equivalent routes in the range from 1 to 32

Defaults	The default is 32 for routers. For switches, it depends on switch models.

Command	
Mode	Global configuration mode

Usage Guide	The number of equivalent routes is configured to control the number of equivalent routes. After the number of equivalent routes is configured by running the maximum-paths command, the number of load-sharing channels in load-sharing mode will not exceed the number of configured static routes. You can run the show running config command to query the number of configured static routes. This command takes effect both to IPv4 and IPv6 addresses. After this command is configured, the maximum number of equivalent routes to an IPv4 or IPv6 destination is equal to the configured value.

Examples	The following example sets the number of equivalent routes to 10 and then restores the default setting. <pre>maximum-paths 10 no maximum-paths 10</pre>

9.14 show ip route

	Use the commands to display the configuration of the IP routing table.	
	show ip route [[vrf <i>vrf_name</i>] [<i>network</i> [<i>mask</i> [longer-prefix]] count <i>protocol</i> [<i>process-id</i>] weight]]	
	show ip route [vrf <i>vrf-name</i>] [[normal ecmp fast-reroute] [<i>network</i> [<i>mask</i>]]	
Parameter Description	Parameter	Description
	vrf <i>vrf_name</i>	(Optional) Displays the route information of the VRF.
	<i>network</i>	(Optional) Displays the route information to the network.
	<i>mask</i>	(Optional) Displays the route information to the network of this mask.
	longer-prefix	(optional) Displays the routes that match the specified prefix.
	count	(Optional) Displays the number of existent routes. (for the ECMP/WCMP route, displays one route)
	<i>protocol</i>	(Optional) Displays the route information of specific protocol.
	<i>process-id</i>	(Optional) Routing protocol process ID.
	weight	(Optional) Displays the route information of non default weight.
	normal	Displays normal routes and not equivalent routes or fast reroutes.

	ecmp	Displays only equivalent routes.
	fast-reroute	(Optional) Displays the master/standby route of fast reroute.

Command Mode	Privileged EXEC mode/ Global configuration mode/Interface configuration mode/ Routing protocol configuration mode/ Route map configuration mode

Usage Guide	This command can display route information flexibly. This command shows all routes. To show different attributes of routes, specify normal ecmp fast-reroute.

Examples	The following example displays the configuration of the IP routing table. <pre>FS# show ip route</pre> Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set <pre>S 20.0.0.0/8 is directly connected, VLAN 1 S 22.0.0.0/8 [1/0] via 20.0.0.1 O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1 R 40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1 B 50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41 C 192.1.1.0/24 is directly connected, VLAN 1 C 192.1.1.254/32 is local host.</pre>
	<pre>FS# show ip route 30.0.0.0</pre> Routing entry for 30.0.0.0/8 Distance 110, metric 20 Routing Descriptor Blocks: <pre>192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2</pre>
	<pre>FS# show ip route count</pre> ----- route info ----- the num of active route: 5
	<pre>FS# show ip route weight</pre> -----[distance/metric/weight]----- <pre>S 23.0.0.0/8 [1/0/2] via 192.1.1.20</pre>


```
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

```
FS#show ip route normal
```

```
Codes: C - Connected, L - Local, S - Static
```

```
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
IA - Inter area, * - candidate default
```

```
Gateway of last resort is no set
```

```
S    20.0.0.0/8 is directly connected, VLAN 1
```

```
S    22.0.0.0/8 [1/0] via 20.0.0.1
```

```
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
```

```
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
```

```
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
```

```
C    192.1.1.0/24 is directly connected, VLAN 1
```

```
C    192.1.1.254/32 is local host
```

```
FS#show ip route ecmp
```

```
Codes: C - Connected, L - Local, S - Static
```

```
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
IA - Inter area, * - candidate default
```

```
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
S*   0.0.0.0/0 [1/0] via 192.168.1.2
```

```
      [1/0] via 192.168.2.2
```

```
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
```

```
      [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

```
FS#show ip route fast-reroute
```

```
Codes: C - Connected, L - Local, S - Static
```

```
R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
IA - Inter area, * - candidate default
```

```
Status codes: m - main entry, b - backup entry, a - active entry
```

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

S* 0.0.0.0/0 [ma] via 192.168.1.2

[b] via 192.168.2.2

O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1

[ba] via 35.1.30.2, 00:38:26, VLAN 3

FS# show ip route fast-reroute 30.0.0.0

Routing entry for 30.0.0.0/8

Distance 110, metric 20

Routing Descriptor Blocks:

[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2

[ba] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20.0.0.0/8	Network address and mask of the destination network
[1/0]	Administrative distance/metric

9.15 show ip route static bfd

Use this command to display the IP route correlated BFD information

show ip route [[vrf vrf_name] static bfd

Parameter	Parameter	Description
Description	vrf <i>vrf-name</i>	(Optional) Displays route information of the specified VRF. The default is global VRF.

Defaults	N/A

Command Mode	Privileged EXEC mode

Usage Guide	Use this command to display the IP route correlated BFD information

Examples	The following example displays the IP route correlated BFD information,	
	FS(config)#show ip route static bfd	
	S 10.0.0.0/8 via 100.100.100.25, GigabitEthernet 0/3, BFD state is Up	
	S 20.0.0.0/8 via 200.100.100.25, GigabitEthernet 0/4, BFD state is Admin	
	Field	Description
	S	Static route
	BFD state	State of the static route correlated BFD.

Related Commands	N/A

Platform Description	This command is not supported on 2-layer devices.

9.16 show ip route summary

	Use this command to display the statistical information about one routing table.
	show ip route [vrf <i>vrf_name</i>] summary
	Use this command to display the statistical information about all routing tables.
	show ip route summary all

Parameter	Parameter	Description
Description	<i>vrf-name</i>	VRF name

Defaults	N/A

Command Mode	Privileged EXEC mode

Usage guideline	N/A

Examples

The following example displays the statistics of the global routing table.

FS# show ip route summary

Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

Memory: 2000 bytes

Entries: 22,based on route prefixes

NORMAL ECMP FRR TOTAL

Connected 3 0 0 3

Static 2 1 1 4

RIP 1 2 1 4

OSPF 2 1 1 4

ISIS 1 2 0 3

BGP 2 1 1 4

TOTAL 11 7 4 22

The following example displays the statistics of all routing tables.

FS# show ip route summary all

Codes: NORMAL – Normal route ECMP – ECMP route FRR – Fast-Reroute route

IP routing table count:2

Total

Memory: 4000 bytes

Entries: 44,based on route prefixes

NORMAL ECMP FRR TOTAL

Connected 6 0 0 6

Static 4 2 2 8

RIP 2 4 2 8

OSPF 4 2 2 8

ISIS 2 4 0 6

BGP 4 2 2 8

TOTAL 22 14 8 44

Global

Memory: 2000 bytes

Entries: 22,based on route prefixes

NORMAL ECMP FRR TOTAL

Connected 3 0 0 3

Static 2 1 1 4

RIP 1 2 1 4

OSPF 2 1 1 4

ISIS 1 2 0 3

BGP 2 1 1 4

TOTAL 11 7 4 22

VRF1 Memory: 2000 bytes Entries: 22,based on route prefixes Entries: 29,based on route nexthops NORMAL ECMP FRR TOTAL Connected 3 0 0 3 Static 2 1 1 4 RIP 1 2 1 4 OSPF 2 1 1 4 ISIS 1 2 0 3 BGP 2 1 1 4 TOTAL 11 7 4 22	
Field	Description
NORMAL	Type of the table entries. Value: NORMAL: common routes (not ECMP or FRR); ECMP: equivalent route; FRR: fast reroute; TOTAL: total
Memory	Memory occupied by the table.
Entries	Number of entries (based on prefix, not next-hop)
Connected	Protocol type. Value: Connected: direct connection; Static: static; RIP: RIP; OSPF: OSPF; ISIS: ISIS; BGP: BGP; TOTAL: total

9.17 show ip route track-table

	Use this command to display the IP route correlated Track information.
	show ip route [[vrf vrf_name] track-table

Parameter	Parameter	Description
Description	vrf vrf_name	(Optional) Displays the route information of the specified VRF name. The default is global VRF,

Defaults	N/A

Command Mode	Privileged EXEC mode

Usage Guide	Use this command to display the IP route correlated Track information.

Examples	The following example displays the IP route correlated Track information.	
	FS(config)#show ip route track-table	
	ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]	
	ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0 2 track 3 state is [down]	
	:	

Field	Description
track	Track target index
state	Track target state

Related	Command	Description
Commands	N/A	N/A

Platform	
Description	This command is not supported on 2-layer devices.

9.18 show ipv6 route

	Use the command to display the configuration of the IPv6 routing table.
	show ipv6 route [[vrf <i>vrf_name</i>] [<i>ipv6-prefix / prefix-length</i> [longer-prefixes] <i>protocol</i> [<i>process-id</i>] weight]]

Parameter Description	Parameter	Description
	vrf <i>vrf-name</i>	(Optional) Specifies a VRF.
	<i>ipv6-prefix/prefix-length</i>	(Optional) Specifies a prefix for route's IPv6 address.
	longer-prefixes	(Optional) Displays the route with an IPv6 address prefix mostly matched.
	<i>protocol</i>	((Optional) Displays the route information of specific protocol.
	<i>process-id</i>	(Optional) Specifies a route process ID.
	weight	(Optional) Displays the non-default-weight routes only.

Defaults	All routes are displayed by default.

Command Mode	Privileged EXEC mode

Usage Guide	Use this command to display route information.

Examples	The following example displays the IPv6 routing table.	
	FS(config)# show ipv6 route	

IPv6 routing table - Default - 7 entries

Codes: C - Connected, L - Local, S - Static

R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

IA - Inter area

C 10::/64 via Loopback 1, directly connected

L 10::1/128 via Loopback 1, local host

S 20::/64 [20/0] via 10::4, Loopback 1C

C FE80::/10 via Null 0, directly connected

C FE80::/64 via Loopback 1, directly connected

L FE80::2D0:F8FF:FE22:33AB/128 via Loopback 1, local host

Field	Description
O	Source routing protocol, which may be: C: directly connected route S: static route R: RIP route B: BGP route O: OSPF route I: IS-IS route
E2	Route type, which may be: E1: OSPF external route type 1 E2: OSPF external route type 2 N1: OSPF NSSA external type 1 N2: OSPF NSSA external type 2 IA: OSPF area internal route SU: IS-IS summary route L1: IS-IS level-1 route L2: IS-IS level-2 route IA: IS-IS area internal route
20::/64	Network address and mask of the destination network
[20/0]	Administrative distance/metric

Related Commands	Command	Description
	ipv6 route	Configures the IPv6 static route.

Platform	
Description	This command is not supported on 2-layer devices.

9.19 show ip route static bfd

	Use this command to display the IPv6 route correlated BFD information
	show ipv6 route [[vrf vrf_name] static bfd

Parameter	Parameter	Description
Description	vrf vrf-name	(Optional) Displays the route information of the designated VRF name of the static route. The default is global VRF,

Defaults	N/A

Command Mode	Privileged EXEC mode

Usage Guide	Use this command to display the IPv6 route correlated BFD information.

Examples

The following example displays the IPv6 route correlated BFD information.

FS(config)#show ip route static bfd

S25::/64 via 100::25, GigabitEthernet 0/3, BFD state is Up

S26::/64 via 200::25, GigabitEthernet 0/4, BFD state is Admin

Field	Description
S	Static route
BFD state	State of the static route associated BFD

Related Commands	N/A

Platform	
Description	This command is not supported on 2-layer devices.

9.20 show ipv6 route summary

	Use this command to display the statistics of the IPv6 routing table of a specified VRF.
	show ipv6 route [vrf vrf-name] summary
	Use this command to display statistics of all IPv6 routing tables.
	show ipv6 route summary all

Parameter	Parameter	Description
Description	vrf-name	(Optional) VRF name. If no VRF name is specified, statistics of the IPv6 routing table of the global VRF are displayed.

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Examples

The following example displays statistics of IPv6 routing table of the global VRF.

```

FS#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected      3
Static         0
PIP            0
OSPF           0
BGP            0
-----
Total          5

```

The following example displays t statistics of all IPv6 routing tables.

```

FS#show ipv6 route summary
IPv6 routing table name is - Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local          2
Connected      3
Static         0
PIP            0
OSPF           0
BGP            0
-----
Total          5

```

Field	Description
Memory	The memory size occupied by the current routing table.
Entries	The entries in the current routing table (based on the entry prefix instead of the next hop entry.)
Connected	Describes the protocol type of the entry. The field can be; Connected: Connected route entry. Static: Static route entry. RIP: RIP route entry. OSPF: OSPF route entry.

		ISIS: ISIS route entry. BGP: BGP route entry. TOTAL: Total number of all protocol entries.	
	IPv6 routing table count	The number of the routing tables.	
	Global	The name of the current routing table. The field can be: Global : Global (The default VRF) VRF1: VRF name. TOTAL: All VRF routing table summaries.	

Related	Command	Description
Commands	N/A	N/A

Platform	
Description	This command is not supported on 2-layer devices.

10 Protocol-independent Commands

10.1 accept-lifetime

	Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its receiving direction. Use the no form of this command to restore the default value.	
	accept-lifetime <i>start-time</i> { infinite <i>end-time</i> duration <i>seconds</i> }	
	no accept-lifetime	
Parameter description	Parameter	Description
	<i>start-time</i>	Start time of the lifetime.
	infinite	Indicates that the encryption key is valid for ever.
	<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
	duration <i>seconds</i>	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.
Default	infinite	
Command mode	Encryption key configuration mode	
Usage guideline	Use this command to specify the lifetime of an encryption key in its receiving direction.	
Examples	The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011. <pre>FS(config)# key chain ripkeys FS(config-keychain)# key 1 FS(config-keychain-key)#accept-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011</pre>	
Related command	Command	Description
	-	-
Platform description	-	

10.2 ip as-path access-list

	Use this command to configure an autonomous system (AS) path filter using a regular expression. Use the no form of this command to remove the AS path filter using a regular expression.	
	ip as-path access-list <i>path-list-num</i> { permit deny } <i>regular-expression</i>	
	no ip as-path access-list <i>path-list-num</i> [{ permit deny } <i>regular-expression</i>]	

Parameter description	Parameter	Description
	<i>path-list-num</i>	Specifies the AS-path access-list number. The range is from 1 to 500.
	permit	Permits advertisement based on matching conditions.
	deny	Denies advertisement based on matching conditions.
	<i>regular-expression</i>	Regular expression that defines the AS-path filter. The expression length range is from 1 to 255 characters.
Default	By default, no AS path filter using a regular expression is configured.	
Command mode	Global configuration mode	
Usage guideline	N/A	
Examples	The following example configures an AS path filter matching the path which contains AS number 123 only. <pre>FS(config)# ip as-path access-list 105 deny ^123\$</pre>	
Related command	Command	Description
	-	-
Platform description	-	

10.3 ip community-list

	Use this command to define a standard or expanded community list and control access to it. Use the no form of this command to remove the setting.
	ip community-list { <i>community-list-number</i> standard <i>community-list-name</i> } { permit deny }
	ip community-list { <i>community-list-number</i> expanded <i>community-list-name</i> } { permit deny } [<i>regular-expression</i>]

Parameter description	Parameter	Description
	standard	Indicates standard community list numbered in 1 to 99.
	expanded	Indicates expanded community list numbered in 100 to 199.
	permit	Permits access to the community list.
	deny	Denies access to the community list.
	<i>community-number</i>	Community number in the form of AA:NN(AS number/2-byte numerical) in the range of 1 to 255 characters. It may also be one of the following value:
Default configuration	None	

Command mode	Global configuration mode.
Usage guidelines	This command is used to define the community list for BGP.
Examples	<pre>FS(config)# ip community-list standard 1 deny 100.20.200.20 FS(config)# ip community-list standard 1 permit internet</pre>

Related commands	Command	Description
	match community	Match the community list.
	set community-list delete	Remove the community value of the BGP path according to the community list.
	show ip community-list	Show the community list information.

10.4 ip extcommunity-list

	Use this command to create an extcommunity list and add an entry to the list. Use the no form of this command to remove the setting.
	ip extcommunity-list { <i>expanded-list</i> expanded <i>list-name</i> } { permit deny } [<i>regular-expression</i>]
	ip extcommunity-list { <i>standard-list</i> standard <i>list-name</i> } { permit deny } [<i>rt value</i>] [<i>soo value</i>]
	no ip extcommunity-list { <i>expanded-list</i> expanded <i>list-name</i> <i>standard-list</i> standard <i>list-name</i> }
	ip extcommunity-list { <i>expanded-list</i> expanded <i>list-name</i> <i>standard-list</i> standard <i>list-name</i> }
	no ip extcommunity-list { <i>expanded-list</i> expanded <i>list-name</i> <i>standard-list</i> standard <i>list-name</i> }

Parameter description	Parameter	Description
	<i>expand-list</i>	Indicates an extended extcommunity list, ranging from 100 to 199. One extcommunity list may contain multiple rules.
	<i>standard-list</i>	Indicates a standard extcommunity list, ranging from 1 to 99. One extcommunity list may contain multiple rules.
	expanded <i>list-name</i>	Indicates the name of an extended extcommunity, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
	standard <i>list-name</i>	Indicates the name of a standard extcommunity list, comprising not more than 32 characters. When using this parameter, you enter the extcommunity list configuration mode.
	permit	Defines an extcommunity rule for permitting.
	deny	Defines an extcommunity rule for denying.
	<i>regular-expression</i>	(optional) Defines a matching template that is used to match an extcommunity.
	<i>sequence-number</i>	(Optional) Defines the sequence number of a rule, ranging from 1 to 2,147,483,647. If no sequence number is specified, the sequence number

		automatically increases by 10 when a rule is added by default. The initial number is 10.
	rt	(Optional) Sets the RT attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
	soo	(Optional) Sets the SOO attribute value. This command can be used only for the standard extcommunity configuration, but not for the extended extcommunity configuration.
	<i>value</i>	Indicates the value of an extended community (extend_community_value).

Default	It is disabled by default.

Command mode	Global configuration mode and ip extcommunity-list configuration mode.

Usage guidelines	This command is used to define the extcommunity list.
Examples	1.The following example defines an ip extcommunity-list. <pre>FS(config)# ip extcommunity-list 1 permit rt 100: 1 FS(config)# ip extcommunity-list standard aaa permit rt 100: 2 FS(config)# ip extcommunity-list expanded ext1 permit 200: [0~9][0~9]</pre>
	2. The following example displays how to use ip extcommunity. <pre>FS(config)# route-map rt_in_filter FS(config-route-map)# match extcommunity 1 FS(config-route-map)# match extcommunity ext1 FS(config)# router bgp 100 FS(config-router)# address-family vpn FS(config-router-af)#neighbor 3.3.3.3 send-community extended FS(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in</pre>

10.5 ip prefix-list

	Use this command to create a prefix list or add an entry to the prefix list. Use the no form of this command to remove the prefix list or an entry.
	ip prefix-list <i>prefix-list-name</i> [seq <i>seq-number</i>] { deny permit } <i>ip-prefix</i> [ge <i>minimum-prefix-length</i>][le <i>maximum-prefix-length</i>]
	no ip prefix-list <i>prefix-list-name</i> [seq <i>seq-number</i>] { deny permit } <i>ip-prefix</i> [ge <i>minimum-prefix-length</i>][le <i>maximum-prefix-length</i>]

Parameter description	Parameter	Description
	<i>prefix-list-name</i>	Name of the prefix list
	<i>seq-number</i>	Sequence number of an entry in the range of 1 to 2147483647. When you execute this command to add an entry without a sequence number, the system allocates a default sequence number for the entry. The default sequence number of the first entry is 5. Every subsequential entry without a sequence number uses the time of 5 larger than the previous sequence number as the default sequence number.
	deny	Deny the route matching the prefix list.
	permit	Permit the route matching the prefix list.
	<i>ip-prefix</i>	Network address and mask. Network address can be any valid IP address and the mask length is in the range of 0 to 32.
	<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of "larger than" and "equivalent to".
	<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of "less than" and "equivalent to".

Default configuration	None

Command mode	Global configuration mode.

Usage guidelines	The ip prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching. You can execute this command to define an exact match, or use "ge" or "le" to define a range match for a prefix for flexible configuration. "ge" indicates the range of minimum-prefix-length to 32; "le" indicates the range of the mask length of the IP prefix to maximum-prefix-length; "ge" and "le" indicates the range of minimum-prefix-length to maximum-prefix-length, namely, mask length of IP prefix < minimum-prefix-length < maximum-prefix-length <=32.

Examples	The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 201.1.1.0/24. <pre> FS# configure terminal FS(config)# ip prefix-list pre1 permit 201.1.1.0/24 FS(config)# router ospf FS(config-router)# distribute-list prefix pre1 out rip FS(config-router)# end </pre>

10.6 ip prefix-list description

	Use this command to add the description of a prefix list. Use the no form of this command to delete the description.
	ip prefix-list <i>prefix-list-name</i> description <i>description-text</i>
	no ip prefix-list <i>prefix-list-name</i> description

Parameter description	Parameter	Description
	<i>prefix-list-name</i>	Name of the prefix list
	<i>description-text</i>	Description of the prefix list

Default configuration	No description is added for a prefix list, by default.

Command mode	Global configuration mode

Examples	The example below adds the description for the prefix list:
	FS# configure terminal
	FS(config)# ip prefix-list <i>pre</i> description Deny routes from Net-A

10.7 ip prefix-list sequence-number

	Use this command to enable sort function for a prefix list. Use the no form of this command to disable the sort function.
	ip prefix-list sequence-number
	no ip prefix-list sequence-number

Parameter description	Disabled

Default configuration	No sequence number is added for a prefix list, by default.

Command mode	Global configuration mode

Examples	The example below adds a sequence number for the prefix list:
	FS# configure terminal
	FS(config)# ip prefix-list <i>pre</i> description deny routes from Net-A

Related commands	Command	Description
	ip prefix-list	Configure the prefix list.

Platform description	N/A

10.8 ipv6 prefix-list

	Use this command to create an IPv6 prefix list or add an entry in the prefix list. Use the no form of this command to delete an IPv6 prefix list or an entry in the prefix list.
	ipv6 prefix-list <i>prefix-list-name</i> [seq <i>seq-number</i>] { deny permit } <i>ipv6-prefix</i> [ge <i>minimum-prefix-length</i>] [le <i>maximum-prefix-length</i>]
	no ipv6 prefix-list <i>prefix-list-name</i> [seq <i>seq-number</i>] { deny permit } <i>ipv6-prefix</i> [ge <i>minimum-prefix-length</i>] [le <i>maximum-prefix-length</i>]

Parameter description	Parameter	Description
	<i>prefix-list-name</i>	Name of the prefix list
	<i>seq-number</i>	Sequence number of an entry in the prefix list. Its range is 1 to 4294967294. If the sequence number is not specified in this command, the system will allocate a default one for the entry. The default sequence number of the first entry is 5, and that of each subsequent one is the product of adding 5 to the sequence number of the proceeding entry.
	permit	Permit the access to the matching result.
	deny	Deny the access to the matching result.
	<i>ipv6-prefix</i>	Network address and its mask. The network address can be any valid IP address. The mask can be 0 to 32 characters.
	<i>minimum-prefix-length</i>	(Optional) Minimum length of the prefix (the starting length) Note: "ge" indicates the operation of "larger than" and "equivalent to".
	<i>maximum-prefix-length</i>	(Optional) Maximum length of the prefix (the ending length) Note: "le" indicates the operation of "less than" and "equivalent to".

Default configuration	No prefix list is created.

Command mode	Global configuration mode

Usage guideline	The ipv6 prefix-list command configures the prefix list, with the permit or deny keyword to determine the action in case of matching. You can execute this command to define an exact match, or use "ge" or "le" to define a range match for a prefix for flexible configuration. "ge" indicates the range of minimum-prefix-length to 128; "le" indicates the range of the mask length of the IP prefix to maximum-prefix-length; "ge" and "le" indicates the range of minimum-prefix-length to maximum-prefix-length, namely, $l_{pv6\text{-}prefix\text{ mask length}} < \text{minimum-prefix-length} < \text{maximum-prefix-length} \leq 128$

Examples	The following example filters the RIP routes the OSPF redistributes by the destination IP address following the rule

defined in the associated IP prefix list, for example, redistribute the routes whose destination IP address is in the range 2222::/64.

```
FS# configure terminal
FS(config)# ipv6 prefix-list pre1 permit 2222::64
FS(config)# ipv6 router ospf
FS(config-router)# distribute-list prefix pre out rip
FS(config-router)# end
```

10.9 ipv6 prefix-list description

Use this command to add the description of an IPv6 prefix list. Use the **no** form of this command to delete the description.

ipv6 prefix-list *prefix-lis-name* **description** *description-text*

no ipv6 prefix-list *prefix-lis-name* **description**

Parameter description	Parameter	Description
	<i>prefix-lis-name</i>	Name of the ipv6 prefix list
	<i>description-text</i>	Description of the ipv6 prefix list

Default

configuration

No description is added for an IPv6 prefix list, by default.

Command

mode

Global configuration mode

Examples

The example below adds the description for the prefix list:

```
FS# configure terminal
FS(config)# ipv6 prefix-list pre description Deny routes from Net-A
```

Related commands	Command	Description
	ipv6 prefix-list	Configure the IPv6 prefix list.

10.10 ipv6 prefix-list sequence-number

Use this command to enable the sorting function for an IPv6 prefix list. Use the **no** form of this command to remove the settings.

ipv6 prefix-list sequence-number

no ipv6 prefix-list sequence-number

Parameter

description

Default

No sequence number is added for a prefix list, by default.

configuration		
Command mode	Global configuration mode	
Examples	The example below adds a sequence number for the prefix list: <pre>FS# configure terminal FS(config)# ipv6 prefix-list pre description Deny routes from Net-A</pre>	
Related commands	Command	Description
	ipv6 prefix-list	Configure the IPv6 prefix list.

10.11 key

	Use this command to define an encryption key and enter the encryption key chain configuration mode. Use the no form of this command to delete it.	
	key <i>key-id</i>	
	no key <i>key-id</i>	
Parameter description	Parameter	Description
	<i>key-id</i>	Key ID, ranging from 0 to 2147483647.
Default	No encryption key is configured.	
Command mode	Encryption key chain configuration mode.	
Usage guideline	Use this command to define an encryption key.	
Examples	The following example configures encryption key chain ripkeys and key 1. <pre>FS(config)# key chain ripkeys FS(config-keychain)# key 1</pre>	
Related command	Command	Description
	-	-
Platform description	-	

10.12 key chain

	Use this command to define a key chain and enter the key chain configuration mode. Use the no form of this command to delete it.	
	key chain <i>key-chain-name</i>	
	no key chain <i>key-chain-name</i>	
Parameter description	Parameter	Description
	<i>key-chain-name</i>	Key chain name.
Default	No key chain is configured.	
Command mode	Global configuration mode.	
Usage guideline	 For a key chain to take effect, you need to configure at least one key.	
Examples	The following example configures key chain ripkeys and enters the key chain configuration mode. <pre>FS(config)# key chain ripkeys</pre>	
Related command	Command	Description
	-	-
Platform description	-	

10.13 key-string

	Use this command to specify a key string. Use the no form of this command to delete it.	
	key-string [0 7] <i>text</i>	
	no key-string	
Parameter description	Parameter	Description
	0	Use plaintext.
	7	Use encryption.
	<i>text</i>	Authentication string.
Default	No key string is configured.	
Command mode	Encryption key configuration mode.	
Usage	Use this command to specify a key string.	

guideline						
Examples	The following example configures key chain ripkeys, key 1 and the key string abc: <pre>FS(config)# key chain ripkeys FS(config-keychain)# key 1 FS(config-keychain-key)#key-string abc</pre>					
Related command	<table><tr><th>Command</th><th>Description</th></tr><tr><td>-</td><td>-</td></tr></table>	Command	Description	-	-	
Command	Description					
-	-					
Platform description	-					

10.14 match as-path

	Use this command to redistribute the routes of AS_PATH attribute permitted by the access list in the route map configuration mode. Use the no form of this command to remove the setting.
	match as-path <i>as-path-acl-list-num</i> [<i>as-path-acl-list-number.....</i>]
	no match as-path [<i>as-path-acl-list-num.....</i>]

Parameter description	Parameter	Description
	<i>as-path-acl-list-num</i>	ACL number, in the range of 1 to 500.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	The match as-path can be followed by an access list number or name. One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	<pre>FS(config)# route-map ROUTEMAP2IBGP FS(config-route-map)# match as-path 20 30</pre>

Related commands	Command	Description
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source of routes.
	set as-path prepend	Set the AS_PATH attribute of redistributed routes
	set metric	Set the metric.

	set metric-type	Set the metric type.

10.15 match community

	Use this command to redistribute the routes matching the Community attribute permitted by the ACL in the route map configuration mode. Use the no form of this command to remove the setting.
	match community { <i>community-list-number</i> <i>community-list-name</i> } [exact-match] [{ <i>community-list-number</i> <i>community-list-name</i> } [exact-match] ...]
	no match community { <i>community-list-number</i> <i>community-list-name</i> } [exact-match] [{ <i>community-list-number</i> <i>community-list-name</i> } [exact-match] ...]

Parameter description	Parameter	Description
	community-list-number	Number of the standard community list in the range 1 to 99. Number of the extended community list in the range of 100 to 199
	community-list-name	Name of the community list in the range of less than 80 characters
	exact-match	Match the community list exactly.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	The match community can be followed by more than one community list number or name, but the total of community lists and names should not be greater than 6. Each exact-match applies to only the previous list, not all the lists. One or more match or set commands can be executed to configure one route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	<pre>FS(config)# ip community-list 1 permit 100:2 100:30 FS(config)# route-map set_lopref FS(config-route-map)# match community 1 exact-match FS(config-route-map)# set local-preference 20</pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.16 match extcommunity

	Use this command to define the match rule for the BGP extcommunity. Use the no form of this command to cancel the setting.	
	match extcommunity { <i>standard-list-number</i> <i>standard-list-name</i> <i>expanded-list-num</i> <i>expanded-list-name</i> }	
	no match extcommunity { <i>standard-list-number</i> <i>standard-list-name</i> <i>expanded-list-num</i> <i>expanded-list-name</i> }	
Parameter description	Parameter	Description
	<i>standard-list-number</i>	Standard extcommunity list number, ranging from 1 to 99. An extcommunity list may contains multiple excommunity values.
	<i>standard-list-name</i>	Standard excommunity name. An extcommunity list may contains multiple excommunity values.
	<i>expanded-list-num</i>	Expanded extcommunity list number, ranging from 100 to 199. An extcommunity list may contains multiple excommunity values.
	<i>expanded-list-name</i>	Expanded excommunity name. An extcommunity list may contains multiple excommunity values.
Default	The rule is not defined in the associated route map.	
Command mode	Route map configuration mode.	
Usage guideline	There are the following scenarios for a route map with an extcommunity: 1. The route map associated with import map uses the RT attribute to filter imported VRF routes. 2. The route maps associated with neighbor route-map in and neighbor route-map out are configured in the BGP VPNv4 address family mode and use the RT attribute to filter VPNv4 routes sent to or by BGP peers.	
Examples	1. Define two extcommunity: <pre>FS(config)# ip extcommunity-list 1 permit rt 100: 1 FS(config)# ip extcommunity-list 1 permit rt 100: 2</pre> 2. Define match rules in the route map: <pre>FS(config)# route-map rt FS(config-route-map)# match extcommunity 1</pre> 3. Use the route map. <pre>FS(config)# router bgp 100 FS(config-router)# address-family vpnv4 FS(config-router-af)# neighbor 3.3.3.3 route-map rt in</pre>	
Related command	Command	Description
	ip extcommunity-list	Create an extcommunity list.
	show ip extcommunity-list	Show an extcommunity list.
Platform description	-	

10.17 match interface

	Use match interface command to redistribute the routes whose next hop is the specified interface. Use the no form of this command to remove the setting.
	match interface <i>interface-type interface-number [...interface-type interface-number]</i>
	no match interface [<i>interface-type interface-number [...interface-type interface-number]</i>]

Parameter description	Parameter	Description
	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface number

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	This command can be followed by multiple interfaces. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map. The following example redistributes the RIP route with the next hop of fastethernet 0/0 in the OSPF routing protocol. <pre> router ospf redistribute rip subnets route-map redrip network 192.168.12.0 0.0.0.255 area 0 route-map redrip permit 10 match interface fastethernet 0/0 </pre>

Related commands	Command	Description
	match ip address	Match the address in the access list.
	match ip next-hop	Match the next-hop IP address in the access list.
	match ip route-source	Match the source IP address in the access list.

	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.18 match ip address

	Use match ip address command to redistribute the routes matching the IP address permitted by the ACL or the prefix list. Use the no form of this command to remove the setting.
	match ip address { <i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] <i>access-list-name</i> [<i>access-list-number...</i> <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]}
	no match ip address [<i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] <i>access-list-name</i> [<i>access-list-number...</i> <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]]

	Parameter	Description
Parameter description	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	Multiple access list numbers or names may follow match ip address. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map. The following example enables the OSPF routing protocol to redistribute RIP routes that match access list 10, with the route type being type-1 external type and the default metric being 40. <pre>router ospf redistribute rip subnets route-map redrip</pre>

```

network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 200.168.23.0 0.0.0.255

route-map redrip permit 10
match ip address 10
set metric 40
set metric-type type-1!

```

Related commands	Command	Description
	access-list	Set the access list.
	match interface	Match the next-hop interface of the route.
	match ip next-hop	Match the next-hop address in the access list.
	match ip route-source	Match the route source address in the access list.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.19 match ip next-hop

	Use match ip next-hop command to redistribute the routes whose next-hop IP address matches the access list or the prefix list. Use the no form of this command to remove the setting.
	match ip next-hop { <i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] [<i>access-list-name</i> [<i>access-list-number...</i>] <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]}
	no match ip next-hop [<i>access-list-number</i> [<i>access-list-number...</i> <i>access-list-name...</i>] [<i>access-list-name</i> [<i>access-list-number...</i>] <i>access-list-name</i>] prefix-list <i>prefix-list-name</i> [<i>prefix-list-name...</i>]]

Parameter description	Parameter	Description
	<i>access-list-number</i>	Number of the access list
	<i>access-list-name</i>	Name of the access list
	<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	Multiple access list numbers or names may follow match ip next-hop. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa.

The mutual route redistribution can be implemented between all the IP routing protocols.

For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains.

One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples

In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the next hop address of the RIP route matches the access list 10 or 20, the OSPF allows for redistribution.

```
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0

access-list 10 permit 192.168.100.1
access-list 20 permit 172.16.10.1

route-map redrip permit 10
 match ip next-hop 10 20
```

Related commands

Command	Description
access-list	Set the access list.
match ip address	Match the IP address in the access list.
match interface	Match the next-hop interface of the route.
match ip route-source	Match the route source address in the access list.
match metric	Match the metric.
match route-type	Match the route type.
match tag	Match the tag.
set metric	Set the metric.
set metric-type	Set the metric type.
set tag	Set the tag.

10.20 match ip route-source

Use **match ip route-source** command to redistribute the routes whose source IP address matches the access list. Use the **no** form of this command to remove the setting.

match ip route-source {*access-list-number* [*access-list-number...* | *access-list-name...*] [*access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]}

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] [*access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]]

Parameter description

Parameter	Description
<i>access-list-number</i>	Number of the access list
<i>access-list-name</i>	Name of the access list
<i>prefix-list prefix-list-name</i>	Specify the prefix list to match.

Default configuration	None.

Command mode	Route map configuration mode.

Usage guidelines	Multiple access list numbers may follow match ip route-source. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	In the example below, the OSPF routing protocol redistributes the RIP routes. As long as the source IP address of the RIP route matches the access list 5, the OSPF allows for redistribution. <pre> router ospf redistribute rip subnets route-map redrip network 192.168.12.0 0.0.0.255 area 0 access-list 5 permit 192.168.100.1 route-map redrip permit 10 match ip route-source 5 </pre>

Related commands	Command	Description
	access-list	Set the access list.
	match ip address	Match the IP address in the access list.
	match interface	Match the next-hop interface of the route.
	match ip next-hop	Match the next-hop IP address in the access list.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.21 match ipv6 address

	Use this command to redistribute the network routes permitted in the IPv6 access list or the IPv6 prefix list. Use the no form of this command to delete the setting. match ipv6 address { <i>access-list-name</i> } prefix-list <i>prefix-list-name</i> }

	no match ipv6 address

Parameter description	Parameter	Description
	<i>access-list-name</i>	Name of the access list.
	prefix-list <i>prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map. The following example enables the OSPF routing protocol to redistribute RIP routes that match access list v6acl, with the default metric being 30. <pre> ipv6 router ospf redistribute rip subnets route-map redrip ipv6 access-list v6acl 10 permit ipv6 2620::64 any route-map redrip permit 10 match ipv6 address v6acl set metric 30 </pre>

Related commands	Command	Description
	ipv6 access-list	Set the IPV6 access list.
	match interface	Match the next-hop interface of the route.
	match ipv6 next-hop	Match the next-hop address in the IPv6 access list.
	match ipvr route-source	Match the route source address in the IPv6 access list.
	match metric	Match the route metric.
	match route-type	Match the route type.
	match tag	Match the route tag.

	set metric	Set the metric for route redistribution.
	set metric-type	Set the type for route redistribution.
	set tag	Set the tag for route redistribution.

10.22 match ipv6 next-hop

	Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the no form of this command to delete the setting. match ipv6 next-hop { <i>access-list-name</i> } prefix-list <i>prefix-list-name</i> } no match ipv6 next hop

Parameter description	Parameter	Description
	<i>access-list-name</i>	Name of the IPv6 access list.
	<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map. The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 40. <pre> ipv6 router ospf redistribute rip subnets route-map redrip ipv6 access-list v6acl 10 permit ipv6 2620::64 any </pre>

```
route-map redrip permit 10
match ipv6 address v6acl
set metric 40
```

Related commands	Command	Description
	ipv6 access-list	Set the IPV6 access list.
	match interface	Match the next-hop interface of the route.
	match ipv6 address	Match the IP address in the IPV6 access list.
	match ipv6 route-source	Match the route source address in the IPV6 access list.
	match metric	Match the route metric.
	match route-type	Match the route type.
	match tag	Match the route tag.
	set metric	Set the metric for route redistribution.
	set metric-type	Set the type for route redistribution.
	set tag	Set the tag for route redistribution.

10.23 match ipv6 route-source

Use this command to redistribute the network routes whose next-hop IP address matches the IPv6 access list or the IPv6 prefix list. Use the **no** form of this command to delete the setting.

match ipv6 route-source { *access-list-name* } | **prefix-list** *prefix-list-name* }

no match ipv6 route-source

Parameter description	Parameter	Description
	<i>access-list-name</i>	Name of the IPv6 access list.
	<i>prefix-list prefix-list-name</i>	Specify the IPv6 prefix list to match.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The route map can be configured very flexibly to be used for route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map. The following example enables the OSPF routing protocol to redistribute RIP routes that only match access list v6acl, with the default metric being 50. <pre> ipv6 router ospf redistribute rip subnets route-map redrip ipv6 access-list v6acl 10 permit ipv6 5200::64 any route-map redrip permit 10 match ipv6 address v6acl set metric 50 </pre>

	Command	Description
Related commands	ipv6 access-list	Set the IPV6 access list.
	match interface	Match the next-hop interface of the route.
	match ipv6 address	Match the IP address in the IPv6 access list.
	match ipv6 next-hop	Match the next hop in the IPv6 access list.
	match metric	Match the route metric.
	match route-type	Match the route type.
	match tag	Match the route tag.
	set metric	Set the metric for route redistribution.
	set metric-type	Set the type for route redistribution.
	set tag	Set the tag for route redistribution.

10.24 match metric

	Use match metric command to redistribute the routes of the specified metric. Use the no form of this command to remove the setting. match metric <i>metric</i> no match metric

Parameter description	Parameter	Description
	<i>metric</i>	Route metric, in the range 0 to 4294967295

Default configuration	None.
Command mode	Route map configuration mode.

Usage guidelines	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	In the example below, the OSPF routing protocol redistributes the RIP routes of metric 10. <pre> router ospf 1 redistribute rip subnets route-map redrip network 192.168.12.0 0.0.0.255 area 0 route-map redrip permit 10 match metric 10 </pre>

Related commands	Command	Description
	access-list	Set the access list.
	match ip address	Match the IP address.
	match interface	Match the interface.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.25 match origin

	Use this command to redistribute the routes whose source IP address is permitted by the ACL in the route map configuration mode. Use the no form of this command to remove the setting. match origin {egp igp incomplete} no match origin [egp igp incomplete]

Parameter description	Parameter	Description
	egp	Redistribute the routes from the remote EGP.
	igp	Redistribute the routes from the local IGP.
	incomplete	Redistribute the routes from an incomplete type.

Default configuration	None

Command	
mode	Route map configuration mode

Usage	
guideline	Use this command to set the origin of the routes to be redistributed. Only one origin can be set.

Examples	<pre> FS(config)# route-map MY_MAP 10 permit FS(config-route-map)# match origin egp FS(config-route-map)# set community 109 FS(config-route-map)# exit FS(config)# route-map MAP20 20 permit FS(config-route-map)# match origin incomplete FS(config-route-map)# set community no-export </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set origin	Set the source.

10.26 match route-type

	Use this command to redistribute the network routes of the specified type. Use the no form of this command to delete the setting. match route-type { static connect rip local internal external [type-1 type-2] level-1 level-2 evpn-type-1 evpn-type-2 evpn-type-3 evpn-type-4 evpn-type-5 } no match route-type [static connect rip local internal external [type-1 type-2] level-1 level-2 evpn-type-1 evpn-type-2 evpn-type-3 evpn-type-4 evpn-type-5]

Parameter description	Parameter	Description
	local	Indicates the local route type.
	static	Indicates the static route type.
	connect	Indicates the directly connected route type.
	rip	Indicates the RIP route type.
	internal	Indicates the OSPF internal route type.
	external	Indicates the OSPF external route type.
	type-1 type-2	Indicates the OSPF type-1 or type-2 route type.
	level-1 level-2	Indicates the ISIS level-1 or level-2 route type.
	evpn-type-1 evpn-type-2 evpn-type-3 evpn-type-4 evpn-type-5	5 route types of BGP EVPN

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	In the example below, the RIP routing protocol redistributes only the internal routes in the OSPF routing domain. <pre> router rip redistribute ospf route-map redrip network 192.168.12.0 route-map redrip permit 10 match route-type internal ! </pre>

Related commands	Command	Description
	access-list	Set the access list.
	match ip address	Match the IP address.
	match interface	Match the interface.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the access list.
	set tag	Match the IP address.

10.27 match tag

	Use this command to redistribute the network routes with the specified tag. Use the no form of this command to delete the setting. match tag <i>tag</i> [...<i>tag</i>] no match tag [<i>tag</i> [...<i>tag</i>]]

Parameter description	Parameter	Description
	<i>tag</i>	Route tag

Default configuration	None
Command mode	Route map configuration mode

Usage guideline	Multiple tags may follow the match tag command. You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	In the example below, the RIP routing protocol redistributes only the routes with tag 50 and 80 in the OSPF routing domain. <pre> FS(config)# router rip FS(config-router)# redistribute ospf 100 route-map redrip FS(config-router)# network 192.168.12.0 FS(config-router)# exit FS(config)# route-map redrip permit 10 FS(config-route-map)# match tag 50 80 </pre>

Related commands	Command	Description
	access-list	Set the access list.
	match ip address	Match the IP address.
	match interface	Match the next-hop IP interface.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match ip next-hop	Match the next-hop IP address.
	match route-type	Match the route type.
	set metric	Set the metric.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.28 memory-lack exit-policy

	Use this command to configure a policy to preferentially exit a routing protocol when the memory reaches the lower limit. Use the no form of this command to restore the default policy, namely, exit the routing protocol which

	occupies the largest memory.	
	memory-lack exit-policy { bgp ospf pim-sm rip }	
	no memory-lack exit-policy	
Parameter description	Parameter	Description
	bgp	Preferentially exit BGP when the memory is insufficient.
	ospf	Preferentially exit OSPF when the memory is insufficient.
	pim-sm	Preferentially exit PIM-SM when the memory is insufficient.
	rip	Preferentially exit RIP when the memory is insufficient.
Default	By default, the routing protocol which occupies the largest memory exits preferentially.	
Command mode	Global configuration mode	
Usage guideline	When the memory reaches the lower limit, you can disable a routing protocol to release the memory to ensure the normal running of other protocols. When the system runs out of memory, disable a routing protocol which has the minimal impact on the system to ensure the operation of main services. Configuring the policy to preferentially exit the routing protocols which are disabled cannot help the system release memory. This command ensures the operation of main services to some extent when the memory is insufficient. If the memory is further consumed, all routing protocols will exit and stop running.	
Examples	The following example configures a policy to preferentially exit the BGP protocol when the memory reaches the lower limit. <pre>FS(config)# memory-lack exit-policy bgp</pre>	
Related command	Command	Description
	-	-
Platform description	-	

10.29 route-map

	Use route-map to enter the route map configuration mode and define a route map. Use the no form of this command to remove the setting. route-map <i>route-map-name</i> [permit deny] [<i>sequence-number</i>] no route-map <i>route-map-name</i> [{permit deny}<i>sequence-number</i>]

Parameter description	Parameter	Description
	<i>route-map-name</i>	Name of the route map. The redistribute command references the route map according to its name. Multiple routing policies can be defined in a route map, and each policy corresponds to one sequence number.
	permit	(Optional) If the permit keyword is defined and the rule defined by match is met, The set command controls the redistributed routes. For policy-based routing, the set command controls the packet forwarding, and exits the route map operation. If the permit keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
	deny	(Optional) If the deny keyword is defined and the rule defined by match is met, no operation will be performed. Neither route redistribution nor policy-based routing is supported in the route map. The system exits the route map operation. If the deny keyword is defined but the rule defined by match is not met, the system performs the routing policy of the second route map till the set command is executed finally.
	<i>sequence-number</i>	Sequence number of the route map. The policy with a lower sequence number is preferred, so it's noted when setting the sequence number.

Default configuration	None.

Command mode	Global configuration mode.

Usage guidelines	At present, the FSOS software primarily uses the route map for route redistribution and policy-based routing. 1. Route redistribution control You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed. When configuring route maps, pay attention to the following when using the sequence number of a route map: When you create the first route map policy, if <i>sequence-number</i> is not specified, it is 10 by default; If only one route map policy exists and <i>sequence-number</i> is not specified, no new route map policy will be created, and the existing route map policy will be accessed for configuration; If more than one route map policy is available, the sequence number of each policy shall be specified; otherwise an error message will be displayed. 2. policy-based routing Policy-based routing refers to a routing mechanism based on user defined policies. Compared with traditional

destination IP address-based routing, policy-based routing offers a flexibility for routing based on source IP address, length and port of IP packets. Policy-based routing can apply to the IP packets received on an interface or the IP packets sent from the local device.

Policy-based routing utilizes route map to define routing and forwarding policy. The match command defines packet filtering rule and the set command defines the action for the packets matching the filtering rules. The match command used includes match ip address and match length; the set command includes set ip tos, set ip precedence, set ip dscp, set ip [default] nexthop, set ip next-hop verify-availability, set [default] interface.

Examples

The following example enables the OSPF routing protocol to redistribute the RIP routes with the hop count of 4. In the OSPF route domain, the route type is the external route type-1, the default metric is 40 and the tag is 40.

```
!
router ospf
 redistribute rip subnets route-map redrip
 network 192.168.12.0 0.0.0.255 area 0
!
!
route-map redrip permit 10
 match metric 4
 set metric 40
 set metric-type type-1
 set tag 40
```

Related commands	Command	Description
	redistribute	Redistribute the routes.

10.30 send-lifetime

Use this command in the encryption key configuration mode to specify the lifetime of an encryption key in its send direction. Use the no form of this command to restore the default value.

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameter description	Parameter	Description
	<i>start-time</i>	Start time of the lifetime.
	infinite	Indicates that the encryption key is valid for ever.
	<i>end-time</i>	<i>End time of the encryption key. It must be later than the start time.</i>
	duration <i>seconds</i>	Duration of the encryption key after the start time. The value ranges from 1 to 2147483646.
Default	infinite	
Command mode	Encryption key configuration mode	

Usage guideline	Use this command to specify the lifetime of an encryption key in its send direction.	
Examples	The following example configures the lifetime from 0:00 on September 9, 2000 to 0:00 on October 12, 2011 FS(config)# key chain ripkeys FS(config-keychain)# key 1 FS(config-keychain-key)# send-lifetime 00:00:00 Sep 9 2000 00:00:00 Dec 12 2011	
Related command	Command	Description
	-	-
Platform description	-	

10.31 set aggregator as

	Use this command to specify the AS_PATH attribute for the aggregator of the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing. set aggregator as <i>as-number ip_addr</i> no set aggregator as [<i>as-number ip_addr</i>]

Parameter description	Parameter	Description
	<i>as-number</i>	AS number of the aggregator.
	<i>ip_address</i>	IP address of the aggregator.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the AS_PATH attribute for the matched routes in the BGP routing domain. Only one group of parameters (as-number, ip-addr) is allowed to set at a time.

Examples	<pre>FS(config)# route-map set-as-path FS(config-route-map)# match as-path 1 FS(config-route-map)# set aggregator as 3 2.2.2.2</pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH.
	match community	Match the community.
	match metric	Match the route metric.

	match origin	Match the route source.
	set community	Set the COMMUNITY attribute.
	set metric	Set the metric.
	set metric-type	Set the type.

10.32 set as-path prepend

	Use this command to specify the AS_PATH attribute for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing. set as-path prepend <i>as-number</i> no set as-path prepend

Parameter description	Parameter	Description
	<i>as-number</i>	Indicates number of the AS_PATH attribute to be configured. The AS number ranges from 1 to 4294967295, and 1 to 65535.65535 in dot mode.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to configure the AS_PATH attribute for the matched routes. Up to 10 ASs can be added into the as-path for one time.

Examples	<pre>FS(config)# route-map set-as-path FS(config-route-map)# match as-path 1 FS(config-route-map)# set as-path prepend 100 101 102</pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH.
	match community	Match the community.
	match metric	Match the route metric.
	match origin	Match the route source.
	set community	Set the COMMUNITY attribute.
	set metric	Set the metric.
	set metric-type	Set the type.

10.33 set atomic-aggregate

	Use this command to set the ATOMIC-AGGREGATE attribute for routes. set atomic-aggregate

	Use the no form of this command to delete existing configuration. no set atomic-aggregate	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Routing map configuration mode	
Default Level	14	
Usage Guide	This command is used only in the BGP protocol and is used to set the ATOMIC-AGGREGATE attribute for routes.	
Configuration Examples	N/A	

10.34 set comm-list delete

	Use this command to delete the COMMUNITY_LIST attribute for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing. set comm-list community-list-number community-list-name delete no set comm-list community-list-number community-list-name delete

Parameter description	Parameter	Description
	<i>community-list-number</i>	Number of the community list. Standard community list number : 1-99. Extended community list number : 100-199.
	<i>community-list-name</i>	Name of the community list, which should be no more than 80 characters.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the community attribute value for the matched routes that will be deleted.

Examples	FS(config)# router bgp 100
	FS(config-router)# neighbor 172.16.233.33 remote-as 120
	FS(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPIN in
	FS(config-router)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out
	FS(config-router)# exit
	FS(config)# ip community-list 500 permit 100:10
	FS(config)# ip community-list 500 permit 100:20
	FS(config)# ip community-list 120 deny 100:50
	FS(config)# ip community-list 120 permit 100:.*
	FS(config)# route-map ROUTEMAPIN permit 10
	FS(config-route-map)# set comm-list 500 delete
	FS(config-route-map)# exit
	FS(config)# route-map ROUTEMAPOUT permit 10
	FS(config-route-map)# set comm-list 120 delete

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute value.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set local-preference	Set the local priority of the route to be redistributed.
	set metric-type	Set the metric type.

10.35 set community

	Use this command to specify the community for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing. set community {community-number[community-number...]} [additive none] no set community

Parameter description	Parameter	Description
	community-number	Community number in the form of AA:NN or a large numeral. In addition, it can be well-known community attributes like internet, local-AS, no-export and no-advertise.
	additive	Increase on the original COMMUNITY attribute.
	none	Set the community attribute as blank.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the community attribute for the matched route.

Examples	<pre> FS(config)# route-map SET_COMMUNITY 10 permit FS(config-route-map)# match as-path 1 FS(config-route-map)# set community 109:10 FS(config-route-map)# exit FS(config)# route-map SET_COMMUNITY 20 permit FS(config-route-map)# match as-path 2 FS(config-route-map)# set community no-export </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH.
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set origin	Set the source.
	set metric-type	Set the metric type.

10.36 set dampening

	Use this command to specify the dampening parameters for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing. set dampening <i>half-life reuse suppress max-suppress-time</i> no set dampening

Parameter description	Parameter	Description
	<i>half-life</i>	Half dampening life for the reachable or unreachable route in the range of 1 to 45 minutes, 15 minutes by default
	<i>reuse</i>	When the route penalty is lower than this value, the route suppression is released. It is in the range 1 to 20000, 750 by default
	<i>suppress</i>	When the route penalty is higher than this value, the route is suppressed. It is in the range 1 to 20000, 2000 by default
	<i>max-suppress-time</i>	Maximum duration a route can be suppressed in the range 1 to 20000 minutes, 4* half-life by default.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the dampening parameter for the matched routes.

Examples	<pre> FS(config)# route-map tag FS(config-route-map)# match as path 10 FS(config-route-map)# set dampening 30 1500 10000 120 FS(config-route-map)# exit FS(config)# router bgp 100 FS(config-router)# neighbor 172.16.233.52 route-map tag in </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH value.
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set local-preference	Set the local priority of the route to be redistributed.

10.37 set extcomm-list delete

	Use this command to delete all extcommunity values in the extcommunity list that meet the match rules. Use the no form of this command to delete the configuration.	
	set extcomm-list { <i>extcommunity-list-number</i> <i>extcommunity-list-name</i> } delete	
	no set extcomm-list { <i>extcommunity-list-number</i> <i>extcommunity-list-name</i> } delete	
Parameter description	Parameter	Description
	<i>extcommunity-list-number</i>	<i>extcommunity-list-number</i> Standard list: ranges from 1 to 99. Expanded list: ranges from 100 to 199.
	<i>extcommunity-list-name</i>	<i>extcommunity-list-name</i> It consists of a maximum of 80 characters.
Default	-	
Command mode	Route map configuration mode.	

Usage guideline	This command is used to delete the extcommunity-list . This command applies only to policy route configuration.																	
Examples	FS(config)# router bgp 65530 FS(config-router)# neighbor 172.16.233.33 remote-as 65531 FS(config-router)# address-family vpnv4 unicast FS(config-router-af)# neighbor 172.16.233.33 activate FS(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPIN in FS(config-router-af)# neighbor 172.16.233.33 route-map ROUTEMAPOUT out FS(config-router)# exit FS(config)# ip extcommunity-list 10 permit rt 100:10 FS(config)# ip extcommunity-list 10 permit rt 100:20 FS(config)# ip extcommunity-list 120 deny 100:50 FS(config)# ip extcommunity-list 120 permit 100:.* FS(config)# route-map ROUTEMAPIN permit 10 FS(config-route-map)# set extcomm-list 10 delete FS(config-route-map)# exit FS(config)# route-map ROUTEMAPOUT permit 10 FS(config-route-map)# set extcomm-list 120 delete																	
Related command	<table><tr><th>Command</th><th>Description</th></tr><tr><td>ip extcommunity-list</td><td>Configure an extcommunity-list.</td></tr><tr><td>match as-path</td><td>Match the AS_PATH value</td></tr><tr><td>match metric</td><td>Match the metric.</td></tr><tr><td>match origin</td><td>Match the source.</td></tr><tr><td>set as-path prepend</td><td>Set the AS_PATH attribute.</td></tr><tr><td>set extcomm-list delete</td><td>Set delete extcommunity-list.</td></tr><tr><td>set local-preference</td><td>Set local preference for a reroute.</td></tr></table>	Command	Description	ip extcommunity-list	Configure an extcommunity-list .	match as-path	Match the AS_PATH value	match metric	Match the metric.	match origin	Match the source.	set as-path prepend	Set the AS_PATH attribute.	set extcomm-list delete	Set delete extcommunity-list .	set local-preference	Set local preference for a reroute.	
Command	Description																	
ip extcommunity-list	Configure an extcommunity-list .																	
match as-path	Match the AS_PATH value																	
match metric	Match the metric.																	
match origin	Match the source.																	
set as-path prepend	Set the AS_PATH attribute.																	
set extcomm-list delete	Set delete extcommunity-list .																	
set local-preference	Set local preference for a reroute.																	
Platform description	-																	

10.38 set extcommunity

	Use this command to specify the extended COMMUNITY attribute for the routes that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.
	set extcommunity {rt <i>extend-community-value</i> soo <i>extend-community-value</i> }
	no set extcommunity {rt soo }

Parameter description	Parameter	Description
	rt	Specify the extended community value in the form of RT.
	soo	Specify the extended community value in the form of SOO.
	<i>extend-community-value</i>	Extended community value.

Default	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the extended community attribute for the matched route.

Examples	<pre>FS(config)# access-list 2 permit 192.168.78.0 255.255.255.0 FS(config)# route-map MAP_NAME permit 10 FS(config-route-map)# match ip-address 2 FS(config-route-map)# set extcommunity rt 100:2</pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH value
	match community	Match the community.
	match metric	Match the metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.39 set fast-reroute

	Use this command to specify a backup outgoing fast reroute and a backup next-hop for routes that meet the match conditions. Use the no form of this command to delete the configuration.	
	set fast-reroute backup-interface <i>interface-type interface-number</i> [backup-nexthop <i>ip-address</i>]	
	no set fast-reroute	
Parameter description	Parameter	Description
	<i>interface-type interface-number</i>	Backup outgoing interface.
	<i>ip-address</i>	Backup next-hop.
Default	-	
Command mode	Route map configuration mode.	
Usage guideline	Use this command to configure IP FRR backup outgoing interface and backup next-hop. The current software version supports only one backup route. This command supports only one set of the two parameters. This command is used for fast reroute configuration.	

	 IP FRR backup routes must not be direct-connection or local host routes.	
Examples	FS(config)# access-list 2 permit 192.168.78.0 255.255.255.0 FS(config)# route-map frr permit 10 FS(config-route-map)# match ip-address 2 FS(config-route-map)# set fast-reroute backup-interface GigabitEthernet 0/1 backup-nexthop 192.168.1.2	
Related command	Command	Description
	match ip-address	Match IP address list.
Platform description	N/A	

10.40 set ip default next-hop

	Use this command to specify the default next-hop IP address for the packets that match the rule in the route map configuration mode. Use the no form of this command to remove the setting.
	set ip default next-hop <i>ip-address</i> [<i>weight</i>] [... <i>ip-address</i> [<i>weight</i>]]
	no set ip default next-hop [<i>ip-address</i> [<i>weight</i>] [... <i>ip-address</i> [<i>weight</i>]]]

Parameter description	Parameter	Description
	<i>ip-address</i>	IP address of the next hop.
	<i>weight</i>	Weight of the next hop.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight inputted. Up to 32 IP addresses may follow the set ip default next-hop command. If a weight follows ip address, up to 4 next hop IP addresses can be configured. Note: If a weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In this mode, the weight of those next hop IP addresses whose weight is not configured is 1 by default. Differences between set ip next-hop and set ip default next-hop: After the set ip next-hop command is configured, the policy-based routing takes precedence over the routing table; while after the set ip default next-hop command is configured, the routing table takes precedence over the policy-based routing. Use this command to customize a default route for a specified user. If the software fails to find the forwarding route, the packet will be forwarded to the nexthop set with this command. To use the policy-based routing, you must specify the route map for it and create the route map. A route map

contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded through the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy. A route-map policy may contain multiple set operations.

Examples

The following example forwards the packets from two different nodes through different routes. For the messages received on the synchronous interface 1 from 1.1.1.1, if the software cannot find the forwarding route, they are forwarded to device 6.6.6.6. For the messages received from 2.2.2.2, if the software cannot find the forwarding route, they are forwarded to device 7.7.7.7. The other messages will be discarded if the software cannot find the forwarding route.

```
FS(config)#access-list 1 permit 1.1.1.1 0.0.0.0
FS(config)#access-list 2 permit 2.2.2.2 0.0.0.0
FS(config)#interface async 1
FS(config-if)#ip policy route-map equal-access
FS(config)#route-map equal-access permit 10
FS(config- route-map)#match ip address 1
FS(config-route-map)#set ip default next-hop 6.6.6.6
FS(config)#route-map equal-access permit 20
FS(config-route-map)#match ip address 2
FS(config-route-map)#set ip default next-hop 7.7.7.7
FS(config)#route-map equal-access permit 30
FS(config- route-map)#set default interface null 0
```

Related commands	Command	Description
	route-map	Define a route map.
	match ip address	Match the IP address.
	set default interface	Set the default outgoing interface.
	set interface	Set the outgoing interface.
	set ip next-hop	Set the next hop of the packets.
	set ip precedence	Set the priority of the packets.

Platform description	N/A

10.41 set ip dscp

	Use this command to specify the DSCP value for the packets that match the rule in the route map configuration mode. Use the no form of this command to remove the setting.
	set ip dscp <i>dscp-value</i>
	no set ip dscp

Parameter description	Parameter	Description
	<i>dscp-value</i>	DSCP value

Default configuration	N/A

Command mode	Route map configuration mode

Usage guideline	N/A

Examples	N/A

Related commands	Command	Description
	route-map	Define a route map.
	match ip address	Match the IP address.
	set default interface	Set the default outgoing interface.
	set interface	Set the outgoing interface.
	set ip next-hop	Set the next hop of the packets.
	set ip precedence	Set the priority of the packets.

10.42 set ip next-hop

	Use this command to specify the next-hop IP address for the packets that meet the matching rule. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.
	set ip next-hop <i>ip-address</i> [<i>weight</i>] [... <i>ip-address</i> [<i>weight</i>]]
	no set ip next-hop [<i>ip-address</i> [<i>weight</i>]] [... <i>ip-address</i> [<i>weight</i>]]

Parameter description	Parameter	Description
	<i>ip-address</i>	Indicates the next-hop IP address.
	<i>weight</i>	Indicates the weight of this next hop.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user. Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32.



If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default.

If weight follows ip address, up to 4 next hop addresses can be configured.

This command can be used to set different routes for the traffic that meets different match rule. If multiple IP addresses are configured, they can be used in turn.

Policy-based routing is a packet forwarding mechanism more flexible than the routing based on the target network. After the policy-based routing is used, the device will decide how to process the packets that need be routed according to the route map, which decides the next-hop device of the packets.

To use the policy-based routing, you must specify the route map for it and create the route map. A route map contains multiple policies, and each policy defines one or more match rules and the corresponding operations. After policy-based routing is applied to an interface, the packets received by the interface will be checked. The packets that do not match any policy in the route map will be forwarded to the usual route. The packets that match a policy in the route map will be processed according to the operation defined in the policy.

A route-map policy may contain multiple set operations.

Examples

The following example enables policy-based routing on serial 1/0. When the interface receives the packets from 10.0.0.0/8, they will be sent to 192.168.100.1; when the interface receives the packets from 172.16.0.0/16, they will be sent to 172.16.100.1; all other packets will be discarded.

```
FS(config)#interface serial 1/0
FS(config-if)#ip policy route-map load-balance
FS(config)#access-list 10 permit 10.0.0.0 0.255.255.255
FS(config)#access-list 20 permit 172.16.0.0 0.255.255
FS(config)#route-map load-balance permit 10
FS(config-route-map)#match ip address 10
FS(config-route-map)#set ip next-hop 192.168.100.1
FS(config)#route-map load-balance permit 20
FS(config-route-map)#match ip address 20
FS(config-route-map)#set ip next-hop 172.16.100.1
FS(config)#route-map load-balance permit 30
FS(config-route-map)#set interface Null 0
```

Related commands

Command	Description
route-map	Define the route map.
match ip address	Match the IP address.
set default interface	Set the default outgoing interface.
set interface	Set the outgoing interface.
set ip default next-hop	Set the default next hop.
set ip precedence	Set the priority of the packets.

10.43 set ip next-hop recursive

	Use this command to specify the recursive next-hop IP address for data packets that match a rule. set ip next-hop recursive <i>ip-address</i>	
	Use the no form of this command to delete the configured next-hop IP address. no set ip next-hop recursive	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Recursive next-hop IP address
Defaults	N/A	
Command Mode	Routing map configuration mode	
Default Level	14	
Usage Guide	This command is used only to configure PBR. Only one set ip next-hop recursive <i>ip-address</i> command can be configured in one routing submap policy. According to the policy, only static or dynamic routes that have an egress and next-hop IP address can be recursed. A route can be recursed to 32 next-hop IP addresses. Only one static route can be recursed to the next hop IP address.	
Examples	The following example enables PBR on Interface serial 1/0. The interface sends the data packets from the source IP address of 10.0.0.0/8 to the recursive next-hop IP address 192.168.100.1, sends the traffic from the source network 172.16.0.0/16 to the recursive next-hop IP address 172.16.100.1, and forwards other data traffic via common routes. <pre> FS(config)#interface serial 1/0 FS(config-if)#ip policy route-map load-balance FS(config)#access-list 10 permit 10.0.0.0 0.255.255.255 FS(config)#access-list 20 permit 172.16.0.0 0.0.255.255 FS(config)#route-map load-balance permit 10 FS(config-route-map)#match ip address 10 FS(config-route-map)#set ip next-hop recursive 192.168.100.1 FS(config)#route-map load-balance permit 20 FS(config-route-map)#match ip address 20 FS(config-route-map)#set ip next-hop recursive 172.16.100.1 </pre>	

10.44 set ip next-hop verify-availability

	Use this command to verify the availability of the next hop IP address for the packets that meet the matching rule.

	Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.
	set ip next-hop verify-availability <i>ip-address</i> [track <i>track-obj-number</i> bfd <i>interface-type interface-number gateway</i>]
	no set ip next-hop verify-availability <i>ip-address</i> [track <i>track-obj-number</i> bfd <i>interface-type interface-number gateway</i>]

Parameter description	Parameter	Description
	<i>ip-address</i>	Indicates the next-hop IP address.
	track	Judges whether the next hop is effective by using <i>Track</i> .
	<i>track-object-num</i>	Indicates the track object number.
	bfd	Indicates that BFD is used for neighbor detection.
	<i>interface-type</i>	Configures the interface type.
	<i>interface-number</i>	Configures the interface number.
	<i>gateway</i>	Configures the gateway IP address, which is the neighbor IP address of BFD. If the next hop is configured as the neighbor, BFD will be used to detect the accessibility of the forwarding path.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	None

Examples	The following example verifies the availability of the next hop IP address being 192.168.1.2 and the number of the object to be tracked to 1.
	FS(config)#route-map <i>rmap</i> permit 10
	FS(config-route-map)#set ip next-hop verify-availability 192.168.1.2 track 1

Related commands	Command	Description
	route-map	Define the route map.
	match ip address	Match the IP address.
	set default interface	Set the default outgoing interface.
	set interface	Set the outgoing interface.
	set ip default next-hop	Set the default next hop.
	set ip precedence	Set the priority of the packets.

10.45 set ip precedence

	Use this command to set the precedence of the IP head of the packet matching the rule in the route map configuration mode. Use the no form of this command to remove the configured precedence setting.
	set ip precedence {<0-7> <i>critical</i> <i>flash</i> <i>flash-override</i> <i>immediate</i> <i>internet</i> <i>network</i> <i>priority</i> <i>routine</i> }
	no set ip precedence

Parameter Description	Parameter	Description
	<i>number</i>	Indicates the priority of the IP header with a number, ranging from 0 to 7. 7: critical 6: flash 5: flash-override 4: immediate 3: internet 2: network 1: priority 0: routine
	critical flash flash-override immediate internet network priority routine	Priority of an IP header.
Defaults	N/A	
Command mode	Route map configuration mode	

Usage guideline	With different precedence values for the IP packet head configured, the IP packets matching the PBR routing are sent according to the different precedence values. Multiple set ip precedence commands can be executed in the route map configuration rule, but only the last one takes effect, and the precedence will be specified for the head of the IP packet matched the PBR.

Examples	The following example sets the precedence of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4: <pre> FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0 FS(config)#route-map name FS(config-route-map)#match ip address 1 FS(config-route-map)#set ip precedence 4 FS(config)#interface FastEthernet 0/0 FS(config-if)#ip policy route-map name </pre>

Related commands	Command	Description
	match interface	Match the next-hop interface.
	match ip address	Match the IP address in the ACL.
	match ip next-hop	Match the next-hop IP address in the ACL.

	match ip route-source	Match the route source IP address in the ACL.
	match metric	Match the route metric value.
	match route-type	Match the route type.
	match tag	Match the route tag value.
	set metric-type	Set the type of redistributed route.
	set tag	Set the tag value of redistributed route.
	set ip tos	Set the tos for the IP packet head.

10.46 set ip tos

	Use this command to set the tos of the IP head of the packet matching the rule in the route map configuration mode. Use the no form of this command to remove the configured tos setting.
	set ip tos {<0-15> <i>max-reliability</i> <i>max-throughput</i> <i>min-delay</i> <i>min-monetary-cost</i> <i>normal</i> }
	no set ip tos

Parameter Description	Parameter	Description
	<i>number</i>	Indicates the TOS value of an IP header with a number, ranging from 0 to 15.
	max-reliability max-throughput min-delay min-monetary-cost normal	Priority of an IP header.
Defaults	N/A	
Command mode	Route map configuration mode	

Usage guideline	With different TOS values for the IP packet head configured, the IP packets matching the PBR routing are transmitted with different service qualities. The TOS value will be specified for the head of the IP packet matched the PBR.

Examples	The following example sets the TOS value of the packet with the source IP address 192.168.217.68 received at the interface FastEthernet 0/0 as 4: <pre> FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0 FS(config)#route-map name FS(config-route-map)#match ip address 1 FS(config-route-map)#set ip tos 4 FS(config)#interface FastEthernet 0/0 FS(config-if)#ip policy route-map name </pre>

Related commands	Command	Description
	match interface	Match the next-hop interface.
	match ip address	Match the IP address in the ACL.
	match ip next-hop	Match the next-hop IP address in the ACL.
	match ip route-source	Match the route source IP address in the ACL.
	match metric	Match the route metric value.
	match route-type	Match the route type.
	match tag	Match the route tag value.
	set metric-type	Set the type of redistributed route.
	set tag	Set the tag value of redistributed route.
	set ip precedence	Set the precedence for the IP packet head.

10.47 set ipv6 default next-hop

	Use this command to specify the default next-hop IPv6 address for the IPv6 packets that match the rule in the route map configuration mode. Use the no form of this command to remove the setting. This command is only used to configure policy-based routing.
	set ipv6 default next-hop <i>global-ipv6-address</i> [<i>weight</i>] [<i>global-ipv6-address</i> [<i>weight</i>] ...]
	no set ipv6 default next-hop <i>global-ipv6-address</i> [<i>weight</i>] [<i>global-ipv6-address</i> [<i>weight</i>] ...]

Parameter description	Parameter	Description
	vrf <i>vrf-name</i>	The next hop address belongs to the specified VRF which must be the configured IPv6 address family multi-protocol VRF.
	global	The next hop address belongs to the global.
	<i>global-ipv6-address</i>	Indicates the next-hop IPv6 address for packet forwarding. The next-hop router must be a neighbor router.
	<i>weight</i>	Indicates the weight in the load balancing mode, ranging from 1 to 8. A larger value means larger packet traffic to be shared by the next hop.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	With the policy-based routing applied to the interface, for the IPv6 packets matching the corresponding rules, if the usual route (that is the non default route) with the destination of this packet is not in the routing table, this packet will be forwarded to the next hop specified by the set ipv6 default next-hop command. Otherwise it is forwarded through the usual route. Noted that the match rule should be the IPv6 corresponded. If the vrf <i>vrf-name</i> parameter is specified, packets are forwarded across different VRF instances. If the global parameter is specified, packets are forwarded from the VRF instance to a public network. If [vrf <i>vrf-name</i> global] is not specified, IPv6 packets are sent to the next hop of the VRF instance same as that of the current hop.

Packets select the egress from the policy-based routing and routing table in following priority:

set ipv6 next-hop;
usual route (the non default route)
set ipv6 default next-hop
default route.



For the switches, this function does not take effect if the mask length is beyond 64.

If this command and the set ipv6 next-hop verify-availability are both configured ,the next hop set by the set ipv6 next-hop verify-availability command will take effect preferentially

Examples

The following examle sets the default next hop of the packet with destination address 2001:0db8:2001:1760::/64 received at the interface fastEthernet 0/0 as 2002:0db8:2003:1::95

```
FS(config)# ipv6 access-list acl_for_pbr
FS(config-ipv6-acl)#permit ipv6 any 2001:0db8:2001:1760::/64
FS(config)#route-map rm_if_0_0
FS(config-route-map)#match ipv6 address acl_for_pbr
FS(config-route-map)# set ipv6 default next-hop
2002:0db8:2003:1::95
FS(config)#interface FastEthernet 0/0
FS(config-if)#ipv6 policy route-map rm_if_0_0
```

Related commands	Command	Description
	match ipv6 address	Set the matching rule of policy-based routing.
	ipv6 policy route-map	Use the policy-based routing on the interface.
	set ipv6 next-hop	Set the next hop of the policy-based routing.

Platform description	N/A

10.48 set ipv6 next-hop

Use this command to specify the next-hop IPv6 address for the packets that meet the matching rule. Use the **no** form of this command to remove the setting. This command is only used to configure policy-based routing.

set ipv6 next-hop *global-ipv6-address* [weight] [...*global-ipv6-address* [weight]]

no set ip next-hop *global-ipv6-address* [weight] [...*global-ipv6-address* [weight]]

Parameter description	Parameter	Description
	<i>global-ipv6-address</i>	IPv6 address of the next hop. The next hop router should be the neighbor

		router.
	<i>weight</i>	Weight of the next hop in the load balancing mode, in the range of 1 to 8.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	This command supports two operation modes: WCMP load balancing mode and non-WCMP load balancing mode. In the former mode, the system implements WCMP load balancing according to the weight entered by the user. Multiple IP addresses may follow set ip next-hop and the number of addresses should be less than 32. If weight follows ip address, up to 4 next hop addresses can be configured. If the parameter <i>vrf vrf-name</i> is specified, packets forwarding will be across the VRF. The packets will be forwarded from VRF to public network with the parameter <i>global</i> specified. If no [<i>vrf vrf-name</i> <i>global</i>] is specified, forwarding the IPv6 packets will inherit the VRF, that is the nexthop belongs to the VRF that receives this IPv6 packets.  If weight follows any next-hop, the operation mode of this command will be automatically switched to the WCMP load balancing mode. In the WCMP load balancing mode, for the nexthop address without configuring the corresponding weight, the weight is 1 by default. When the packets select the egress from the policy-based routing and routing table, the priorities are as follows. - set ipv6 next-hop; - usual route (the non default route) - set ipv6 default next-hop - Default route.

Examples	The following example sets the next hop of the packet with destination address <i>2001:0db8:2001:1760::/64</i> received at the interface <i>fastEthernet 0/0</i> as <i>2002:0db8:2003:1::95</i> <pre> FS(config)# ipv6 access-list <i>acl_for_pbr</i> FS(config-ipv6-acl)# permit ipv6 any <i>2001:0db8:2001:1760::/64</i> FS(config)# route-map <i>rm_if_0_0</i> FS(config-route-map)# match ipv6 address <i>acl_for_pbr</i> FS(config-route-map)# set ipv6 next-hop <i>2002:0db8:2003:1::95</i> FS(config)# interface FastEthernet 0/0 FS(config-if)# ipv6 policy route-map <i>rm_if_0_0</i> </pre>

Related commands	Command	Description
	match ipv6 address	Set the matching rule of policy-based routing.
	ipv6 policy route-map	Use the policy-based routing on the interface.

	set ipv6 next-hop	Set the next hop of the policy-based routing.

Platform description	N/A

10.49 set ipv6 next-hop verify-availability

	Use this command to determine the availability of the next-hop IP address. set ipv6 next-hop verify-availability <i>global-ipv6-address</i> [track <i>track-obj-number</i> bfd <i>interface-type interface-number gateway</i>]	
	Use the no form of this command to delete existing configuration. no set ip next-hop verify-availability <i>global-ipv6-address</i> [track <i>track-obj-number</i> bfd <i>interface-type interface-number gateway</i>]	
Parameter Description	Parameter	Description
	<i>global-ipv6-address</i>	Specifies the next-hop IPv6 address.
	track	Detects whether the next hop is effective by using the tracking method.
	<i>track-obj-number</i>	Specifies the tracking object number.
	bfd	Conducts neighbor detection by using BFD.
	<i>interface-type</i>	Specifies the interface type.
	<i>interface-number</i>	Specifies the interface number.
	<i>gateway</i>	Specifies the gateway IPv6 address, that is, IPv6 address of the BFD neighbor. If the configured next hop is the neighbor, the availability of the forwarding path will be detected using BFD.
Defaults	N/A	
Command Mode	Routing map configuration mode	
Default Level	14	
Usage Guide	This command is used only to configure PBR.	
Examples	The following example enables the PBR support for BFD and detects the forwarding path to the neighbor 2001:1::2 via BFD. <pre>FS(config)# route-map rmap permit 10 FS(config-route-map)# set ipv6 next-hop verify-availability 2001:1::2 bfd FastEthernet 0/1 2001:1::2</pre>	

10.50 set ipv6 precedence

	Use this command to set the precedence of the IPv6 head of the packet matching the rule in the route map

	configuration mode. Use the no form of this command to remove the configured precedence setting.
	set ipv6 precedence {number <i>critical</i> <i>flash</i> <i>flash-override</i> <i>immediate</i> <i>internet</i> <i>network</i> <i>priority</i> <i>routine</i> }
	no set ipv6 precedence

Parameter description	Parameter	Description
	<i>critical</i> , <i>flash</i> , <i>flash-override</i> , <i>immediate</i> , <i>internet</i> , <i>network</i> , <i>priority</i> , <i>routine</i>	The precedence type of the IPv6 head.
	number	The configurable precedence range.

Default configuration	N/A

Command mode	Route map configuration mode

Usage guideline	

Examples	The following example sets the precedence of IPv6 packet head as 3: Configure route-map.
	FS(config)#route-map <i>pbr-aaa</i> permit 10
	FS(config-route-map)# set ipv6 precedence 3
	Or
	FS(config-route-map)# set ipv6 precedence immediate

Related commands	Command	Description
	match ipv6 address	Configure the ACL used for matching the packet in IPv6 PBR.
	route-map	Use the route map of the policy-based routing.
	set default interface	Set the default next-hop egress.
	set interface	Set the next hop egress.
	set ipv6 default next-hop	Set the default next-hop address for forwarding packets.
	set ipv6 next-hop	Set the next-hop address for forwarding packet.
	show ipv6 policy	Show the policy-based routing
	show route-map	Show the route map configuration.

Platform description	N/A

10.51 set level

	Use this command to set the level of the area where the routes matching the rule are redistributed in the route map configuration command. Use the no form of this command to remove the setting.

	set level {level-1 level-2 level-1-2 stub-area backbone}	
	no set level	
Parameter Description	Parameter	Description
	level-1	Indicates that the re-distribution route is advertised to ISIS Level 1.
	level-2	Indicates that the re-distribution route is advertised to ISIS Level 2.
	level-1-2	Indicates that the re-distribution route is advertised to ISIS Level 1 and Level 2.
	stub-area	Indicates that the re-distribution route is advertised to OSPF Stub Area.
	backbone	Indicates that the re-distribution route is advertised to the OSPF backbone area.

Default configuration	None

Command mode	Route map configuration mode

Examples	In the example below, the OSPF routing protocol redistributes the RIP protocol to the backbone area. <pre> FS(config)# router ospf FS(config-router)# redistribute rip subnets route-map <i>redrip</i> FS(config-router)# network 192.168.12.0/24 area 0 FS(config-router)# exit FS(config)# route-map <i>redrip</i> permit 10 FS(config-route-map)# set level backbone </pre>

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.52 set local-preference

	Use this command to set the LOCAL PREFERENCE value for the routes to be redistributed in the route map configuration mode. Use the no form of this command to remove the setting.
	set local-preference <i>number</i>
	no set local-preference

Parameter description	Parameter	Description
	<i>number</i>	Local priority metric ranging 1 to 4294967295

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the local preference for the matched routes. Only one local preference can be set.

Examples	<pre> FS(config)# route-map SET_PREF permit 10 FS(config-route-map)# match as-path 1 FS(config-route-map)# set local-preference 6800 FS(config-route-map)# exit FS(config)# route-map SET_PREF permit 20 FS(config-route-map)# match as-path 2 FS(config-route-map)# set local-preference 50 </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match metric	Match the route metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.53 set metric

	Use set metric to set the metric for the routes to be redistributed. Use the no form of this command to remove the setting.
	set metric [+ <i>metric-value</i> - <i>metric-value</i> <i>metric-value</i>]
	no set metric

Parameter description	Parameter	Description
	+	Increase based on the metric of the original route
	-	Decrease based on the metric of the original route
	<i>metric-value</i>	Metric for the route to be redistributed

Default configuration	The default metric for route redistribution varies with the routing protocol.

Command mode	Route map configuration mode

Usage guideline	You should set the metric according to the actual network topology, because the routing depends on the metric of routes. Attentions should be paid to the upper and lower limits of the routing protocols when you execute the set metric, + metric or – metric commands. When the RIP protocol redistributes the routes of other protocols, the range of the metric after increase or decrease is 1 to 16. You can redistribute the routes from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. For route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. One or more match or set commands can be executed to configure a route map. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The following example enables the OSPF routing protocol to redistribute the RIP routes and sets the default metric to 40. <pre> FS(config)# router ospf FS(config-router)# redistribute rip subnets route-map redrip FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 FS(config-router)# exit FS(config)# route-map redrip permit 10 FS(config-route-map)# set metric 40 </pre>

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.54 set metric-type

	Use set metric-type to set the type of the routes to be redistributed. Use the no form of this command to remove the setting.
	set metric-type <i>type</i>
	no set metric-type

Parameter description	Parameter	Description
	<i>type</i>	Type of the routes to be redistributed. At present, you can set the type of the routes that the OSPF protocol redistributes.

Default configuration	

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols.
	In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The following example enables the OSPF routing protocol to redistribute the RIP route and sets the type as type-1.
	<pre> FS(config)# router ospf FS(config-router)# redistribute rip subnets route-map <i>redrip</i> FS(config-router)# network 192.168.12.0/24 area 0 FS(config-router)# exit FS(config)# route-map <i>redrip</i> permit 10 FS(config-route-map)# set metric-type type-1 </pre>

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set tag	Set the tag.

10.55 set next-hop

	Use this command to specify the next-hop IP address for the routes that match the rule. Use the no form of this

	command to remove the setting. This command is only used to configure routing policies.
	set next-hop <i>ip-address</i>
	no set next-hop

Parameter	Parameter	Description
description	<i>ip-address</i>	IP address of the next hop.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	You can redistribute the routing information from one routing process to another routing process. For example, you can redistribute the route in the OSPF routing domain and then advertise it to the RIP routing domain, and vice versa. The mutual route redistribution can be implemented between all the IP routing protocols. In the route redistribution, route maps are usually used to control the mutual route redistribution between two routing domains. In configuring one route map, one or more match or set commands can be executed. If the match command is not used, all the routes will be matched. If the set command is not used, no operation will be performed.

Examples	The following example enables the OSPF routing protocol to redistribute the RIP route and sets the next-hop to 192.168.1.2. <pre>FS(config)# route-map redrip permit 10 FS(config-route-map)# match ip address 1 FS(config-route-map)# set next-hop 192.168.1.2</pre>

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric-type	Set the metric type.
	set tag	Set the tag.

10.56 set origin

	Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the no form of this command to remove the setting.

	set origin {egp igp incomplete}
	no set origin

Parameter description	Parameter	Description
	egp	Redistribute the routes from the remote EGP.
	igp	Redistribute the routes from the local IGP.
	incomplete	Redistribute the routes from an unknown device.

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	Use this command to set the source of the routes to be matched. Only one route source attribute can be set.

Examples	<pre> FS(config)# route-map SET_ORIGIN 10 permit FS(config-route-map)# match as-path 1 FS(config-route-map)# set origin igp FS(config-route-map)# exit FS(config)# route-map SET_ORIGIN 20 permit FS(config-route-map)# match as-path 2 FS(config-route-map)# set origin egp </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match metric	Match the route metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set local-preference	Set the local priority of redistributed routes.

10.57 set originator-id

	Use this command to set the source of the routes to be redistributed in the route map configuration mode. Use the no form of this command to remove the setting.
	set originator-id <i>ip-address</i>
	no set originator-id [<i>ip-address</i>]

Parameter description	Parameter	Description
	<i>ip-address</i>	IP address of the originator.

Default configuration	None
Command mode	Route map configuration mode
Usage guideline	Use this command to set the source of the routes to be matched.
Examples	<pre> FS(config)# route-map SET_ORIGIN 10 permit FS(config-route-map)# match as-path 1 FS(config-route-map)# set originator-id 5.5.5.5 FS(config-route-map)# exit FS(config)# route-map SET_ORIGIN 20 permit FS(config-route-map)# match as-path 2 FS(config-route-map)# set originator-id 5.5.5.6 </pre>

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match metric	Match the route metric.
	match origin	Match the source.
	set as-path prepend	Set the AS_PATH attribute.
	set metric	Set the metric.
	set local-preference	Set the local priority of redistributed routes.

10.58 set tag

	Use this command to set the tag for the routes to be redistributed. Use the no form of this command to remove the setting.
	set tag tag
	no set tag

Parameter	Parameter	Description
description	tag	Tag of the route to be redistributed

Default configuration	The original routing tag remains unchanged.
Command mode	Route map configuration mode
Usage guideline	This command can only be used for route redistribution. If this command is not configured, the default route tag is used.

Examples	The following example enables the OSPF routing protocol to redistribute the RIP route and sets the tag as 100.
	<pre> FS(config)# router ospf FS(config-router)# redistribute rip subnets route-map redrip FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 FS(config-router)# exit FS(config)# route-map redrip permit 10 FS(config-route-map)# set tag 100 </pre>

Related commands	Command	Description
	match interface	Match the interface.
	match ip address	Match the IP address.
	match ip next-hop	Match the next-hop IP address.
	match ip route-source	Match the source IP address.
	match metric	Match the metric.
	match route-type	Match the route type.
	match tag	Match the tag.
	set metric	Set the metric.
	set metric-type	Set the metric type.

10.59 set weight

	Use this command to set the weight for the BGP routes matching filtering rules. Use the no form of this command to remove the setting.
	set weight <i>number</i>
	no set weight

Parameter description	Parameter	Description
	<i>number</i>	Weight in the range of 0 to 65535

Default configuration	None

Command mode	Route map configuration mode

Usage guideline	This command can only be used modify the weight of a BGP route. By default, the weight of the route learned from a neighbor is the one configured with the neighbor weight command. The weight of the locally generated route is fixed 32768.

Examples	The following example sets the weight for the BGP route learned from the neighbor 1.1.1.1 at the inbound direction to 100.

```

FS(config)# router bgp 1
FS(config-router)# neighbor 1.1.1.1 route-map nei-rmap-in in
FS(config-router)# exit
FS(config)# route-map nei-rmap-in permit 10
FS(config-route-map)# set weight 100

```

Related commands	Command	Description
	match as-path	Match the AS_PATH attribute.
	match community	Match the route community.
	match metric	Match the route metric.
	match origin	Match the source.
	set community	Set community of the redistributed route.
	set metric	Set the metric of the redistributed route.
	set metric type	Set the metric type of the redistributed route.

10.60 show ip as-path-access-list

	Use this command to display the configuration of AS path access lists.	
	show ip as-path-access-list [<i>num</i>]	
Parameter description	Parameter	Description
	<i>num</i>	AS path access list number.
Default	N/A	
Command mode	Privileged EXEC mode	
Usage guideline	N/A	
Examples	The following example displays the AS path access lists.	
	<pre> FS# show ip as-path-access-list AS path access list 30 permit ^30\$ </pre>	
	Field	Description
	AS path access list	AS path access list number
	permit	Permits advertisement based on matching conditions.
	^30\$	Regular expression.

Related command	Command	Description
	-	-
Platform description	-	

10.61 show ip community-list

	Use show ip community-list command to display the community list.
	show ip community-list [<i>community-list-number</i> <i>community-list-name</i>]

Parameter description	Parameter	Description
	<i>community-list-number</i>	Number of the community list.
	<i>community-list-name</i>	Name of the community list.

Default configuration	None

Command mode	Privileged EXEC mode

Usage guidelines	N/A

Examples	<pre> FS# show ip community-list Community-list standard local permit local-AS Community-list standard Red-Giant permit 0:10 deny 0:20 </pre>

Related commands	Command	Description
	match community	Match the route community.
	set comm-list delete	Delete the community attribute in the BGP routes.

10.62 show ip extcommunity-list

	Use this command to display the extcommunity list.	
	show ip extcommunity-list [<i>extcommunity-list-num</i> <i>extcommunity-list-name</i>]	
Parameter description	Parameter	Description
	<i>extcommunity-list-num</i>	extcommunity-list number, ranging from 1 to 199.
	<i>extcommunity-list-name</i>	extcommunity-list name.

Default	-	
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode and route map configuration mode.	
Usage guideline	-	
Examples	FS # show ip extcommunity-list Standard extended community-list 1 10 permit RT:1:200 20 permit RT:1:100 Standard extended community-list 2 10 permit RT:1:200 Expanded extended community-list rt_filter 13 permit 1:100	
Related command	Command	Description
	ip extcommunity-list	Create an extcommunity-list.
	match extcommunity	Match an extcommunity.
	set extcommunity	Set an extcommunity.
Platform description	-	

10.63 show ip prefix-list

	Use show ip prefix-list to display the prefix list or the entries.
	show ip prefix-list [<i>prefix-name</i>]

Parameter description	Parameter	Description
	<i>prefix-name</i>	Name of the prefix list.

Default configuration	The configuration information of all the prefix lists is displayed by default.

Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines	If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples	<pre>FS# show ip prefix-list seq pre: 2 entries seq 5 permit 192.168.564.0/24 seq 10 permit 192.2.2.0/24</pre>

10.64 show ip protocols

	Use this command to display information about the status of the currently running IPv4 routing protocol. show ip protocols [vrf vrf-name] { bgp isis ospf rip }	
Parameter Description	Parameter	Description
	vrf-name	Specifies the VRF instance name. If it is not specified, information about the status of routing protocols in global VRF mode is displayed.
	bgp	Displays information about the status of the BGP protocol.
	isis	Displays information about the status of the IS-IS protocol.
	ospf	Displays information about the status of the OSPF protocol.
	rip	Displays information about the status of the RIP protocol.
	-	Displays information about the status of all running routing protocols.
Command Mode	Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and routing map configuration mode	
Default Level	14	
Usage Guide	Information about the status of only the currently running routing protocol is displayed, and the information about a routing protocol that is not running is not displayed.	
Examples	The following example displays the status of routing protocols running in global VRF mode. <pre>FS# show ip protocols Routing Protocol is "ospf 1" Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Router ID 57.57.57.57 Memory Overflow is enabled Router is not in overflow state now It is an autonomous system boundary router Redistributing External Routes from, connected, includes subnets in redistribution bgp, includes subnets in redistribution Number of areas in this router is 2: 2 normal 0 stub 0 nssa Routing for Networks:</pre>	


```

57.57.57.57 0.0.0.0 area 0
163.18.4.0 0.0.0.255 area 0
163.18.57.0 0.0.0.255 area 0
192.100.1.0 0.0.0.255 area 0
192.101.1.0 0.0.0.255 area 1
192.102.1.0 0.0.0.255 area 0
Reference bandwidth unit is 100 mbps
Distance: (default is 110)

Routing Protocol is "bgp 10"
IGP synchronization is disabled
Default-information originate is disabled
Default local-preference applied to incoming route is 100
Redistributing: connected
Neighbor(s):
  Address          AddressFamily  FiltIn  FiltOut  DistIn  DistOut  RouteMapIn  RouteMapOut
Weight
Distance: external 20(default) internal 200(default) local 200(default)

```

Field description:

Field	Description
Routing Protocol is "ospf 1"	Name of a routing protocol
Redistributing External Routes from	Route redistribution status of a routing protocol
Distance:	Distance information of a routing protocol

10.65 show ipv6 prefix-list

Use this command to display the information about the IPv6 prefix list or its entries.

show ipv6 prefix-list [*prefix-name*]

Parameter	Parameter	Description
description	<i>prefix-name</i>	Name of the IPv6 prefix list.

Default configuration	The configuration information of all the IPv6 prefix lists is displayed.

Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, route protocol configuration mode, route map configuration mode

Usage guideline	If no prefix list is specified, the configurations of all the prefix lists are displayed, otherwise only the configuration of the specified prefix list is displayed.

Examples	<pre> FS# show ipv6 prefix-list ipv6 prefix-list p6: 2 entries seq 5 permit 13::/20 seq 10 permit 14::/20 </pre>

10.66 show key chain

	Use this command to display the key chain configuration.	
	show key chain [<i>key-chain-name</i>]	
Parameter description	Parameter	Description
	key-chain-name	(Optional) Display the configuration of the specified key chain.
Default	The configuration information of all key chains is displayed.	
Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, and key chain configuration mode.	
Usage guideline	If no key chain is specified, the configuration information of all key chains is displayed.	
Examples	FS# show key chain route-map AAA, permit, sequence 10 Match clauses: ip address 2 Set clauses: metric 10 FS(config)#show key chain key chain kc key 1 -- text "FS" accept-lifetime (12:11:00 May 2 2001) - (infinite) send-lifetime (always valid) - (always valid) [valid now]	
	Field	Description
	key chain	Key chain name.
	key	Key ID.
	accept-lifetime	Lifetime in the accept direction.
	send-lifetime	Lifetime in the send direction.
Related command	Command	Description
	-	-
Platform	-	

description	

10.67 show route-map

	Use the command to display the configuration of the route map.
	show route-map [<i>route-map-name</i>]

Parameter	Parameter	Description
description	<i>route-map-name</i>	(Optional) Display the configuration information of the specified the route map.

Default configuration	The configuration information of all the route maps is displayed.

Command mode	Privileged EXEC mode, global configuration mode, interface configuration mode, routing protocol configuration mode, route map configuration mode.

Usage guidelines	If no route map is specified, the configurations of all the route maps will be displayed, otherwise only the configuration of the specified route map is displayed.

Examples	<pre>FS# show route-map route-map AAA, permit, sequence 10 Match clauses: ip address 2 Set clauses: metric 10</pre>	
	Field	Description
	route-map	Name of the route map.
	Permit	The route map contains the permit keyword.
	sequence 10	Sequence number of the route map.
	Match clauses	Set the matching rule. Whether to perform the set operation depends on the permit or deny keyword in the route map.
	Set clauses	Set the operation when the rule is matched.

Security Configuration Commands

AAA Commands

1.1 bandwidth

	Use this command to configure NAS command accounting. Use the no form of this command to restore the default setting.	
	aaa accounting commands <i>level</i> { default <i>list-name</i> } start-stop <i>method1</i> [<i>method2...</i>]	
	no aaa accounting commands <i>level</i> { default <i>list-name</i> }	
Parameter Description	Parameter	Description
	<i>level</i>	The accounting command level, 0-15. The message shall be recorded before which command level is executed is determined.
	default	When this parameter is used, the following defined method list is used as the default method for command accounting.
	<i>list-name</i>	Name of the command accounting method list, which could be any character strings.
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the TACACS+ server group is supported.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS enables the accounting command function after enabling the login authentication. After enabling the accounting function, it sends the command information to the security service. The configured accounting command method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.	
Configuration Examples	The following example enables NAS command accounting. <pre>FS(config)# aaa accounting commands 15 default start-stop group tacacs+</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authentication	Defines AAA authentication.
	accounting commands	Applies the accounting commands to the terminal

		line.
Platform	N/A	
Description		

1.2 aaa accounting exec

	Use this command to enable NAS access accounting. Use the no form of this command to restore the default setting.	
	aaa accounting exec { default list-name } start-stop method1 [method2...]	
	no aaa accounting exec { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined method list is used as the default method for Exec accounting.
	<i>list-name</i>	Name of the Exec accounting method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: none and group . One method list can contain up to four methods.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS enables the exec accounting function after enabling the login authentication. After enabling the accounting function, it sends the account start information to the security server when the users log in the NAS CLI, and sends the account stop information to the security server when the users log out. If it does not send the account start information to the security server when a user logs in, it does not send the account stop information to the security server when a user logs out, either. The configured exec accounting method must be applied to the terminal line that needs accounting command; otherwise it is ineffective.	
Configuration Examples	The following example enables NAS access accounting. <pre>FS(config)# aaa accounting network start-stop group radius</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authentication	Defines AAA authentication.
	accounting commands	Applies the Exec accounting to the terminal line.

Platform	N/A
Description	

1.3 aaa accounting network

	Use this command to enable network access accounting. Use the no form of this command to restore the default setting.	
	aaa accounting network { default list-name } start-stop method1 [method2..]	
	no aaa accounting network { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined method list is used as the default method for Network accounting.
	<i>list-name</i>	Name of the accounting method list
	<i>method</i>	Sends accounting messages at both the start time and the end time of access. Users are allowed to access the network, no matter whether the start accounting message enables the accounting successfully.
	none	Does not perform accounting.
	group	Uses the server group for accounting, the RADIUS and TACACS+ server group is supported.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS performs accounting of user activities by sending record attributes to the security server. Use the start-stop keyword to set the user accounting option.	
Configuration Examples	The following example enables network access accounting.	
	FS(config)# aaa accounting network start-stop group radius	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization network	Defines a network authorization method list.
	aaa authentication	Defines AAA authentication.
	username	Defines a local user database.
Platform	N/A	
Description		

1.4 aaa accounting update

	Use this command to enable the accounting update function.

	Use the no form of this command to restore the default setting.	
	aaa accounting update	
	no aaa accounting update	
Parameter Description	N/A	
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.	
Configuration Examples	The following example enables the accounting update function. <pre>FS(config)# aaa new-model FS(config)# aaa accounting update</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa accounting network	Defines a network accounting method list.
Platform Description	N/A	

1.5 aaa accounting update periodic

	Use this command to set the interval of sending the accounting update message.	
	Use the no form of this command to restore the default setting.	
	aaa accounting update periodic <i>interval</i>	
	no aaa accounting update periodic	
Parameter Description	Parameter	Description
	<i>interval</i>	Interval of sending the accounting update message, in the unit of minutes. The shortest interval is 1 minute.
Defaults	The default is 5 minutes.	
Command Mode	Global configuration mode	
Usage Guide	If the AAA security service is not enabled, the accounting update function cannot be used. This command is used to set the accounting interval if the AAA security service has been enabled.	

Configuration	The following example sets the interval of accounting update to 1 minute.							
Examples	<pre>FS(config)# aaa new-model FS(config)# aaa accounting update FS(config)# aaa accounting update periodic 1</pre>							
Related								
Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>aaa new-model</td><td>Enables the AAA security service.</td></tr><tr><td>aaa accounting network</td><td>Defines a network accounting method list.</td></tr></table>	Command	Description	aaa new-model	Enables the AAA security service.	aaa accounting network	Defines a network accounting method list.	
Command	Description							
aaa new-model	Enables the AAA security service.							
aaa accounting network	Defines a network accounting method list.							
Platform	N/A							
Description								

1.6 aaa authentication dot1x

	Use this command to enable AAA authentication 802.1x and configure the 802.1x user authentication method list. Use the no form of this command to delete the 802.1x user authentication method list.	
	aaa authentication dot1x { default <i>list-name</i> } <i>method1</i> [<i>method2</i> ...]	
	no aaa authentication dot1x { default <i>list-name</i> }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined 802.1x user authentication method list is used as the default method for user authentication.
	list-name	Name of the 802.1x user authentication method list, which could be any character string
	method	It must be one of the keywords: local , none and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS server group is supported.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the AAA 802.1x security service is enabled on the device, users must use AAA for 802.1x user authentication negotiation. You must use the aaa authentication dot1x command to configure a default or optional method list for 802.1x user authentication. The next method can be used for authentication only when the current method does not work.	
Configuration	The following example defines an AAA authentication method list named RDS_D1X . In the authentication	

Examples	method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.	
	FS(config)# aaa authentication dot1x rds_d1x group radius local	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	dot1x authentication	Associates a specific method list with the 802.1x user.
	username	Defines a local user database.
Platform Description	N/A	

1.7 aaa authentication enable

	Use this command to enable AAA Enable authentication and configure the Enable authentication method list. Use the no form of this command to delete the user authentication method list.	
	aaa authentication enable default <i>method1</i> [<i>method2...</i>]	
	no aaa authentication enable default	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for Enable authentication.
	<i>method</i>	It must be one of the keywords: local , none and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.
	enable	Enables AAA Enable authentication.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the AAA Enable authentication service is enabled on the device, users must use AAA for Enable authentication negotiation. You must use the aaa authentication enable command to configure a default or optional method list for Enable authentication. The next method can be used for authentication only when the current method does not work. The Enable authentication function automatically takes effect after configuring the Enable authentication method list.	
Configuration Examples	The following example defines an AAA Enable authentication method list. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local	

	user database is used for authentication. FS(config)# aaa authentication enable default group radius local	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	enable	Switchover the user level.
	username	Defines a local user database.
Platform Description	N/A	

1.8 aaa authentication iportal

	Use this command to enable AAA Portal Web user authentication. Use the no form of this command to delete the authentication method list.	
	aaa authentication iportal { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	
	no aaa authentication iportal { default <i>list-name</i> }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: local , none , subs and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS server group is supported.
	subs	Uses the subs database for authentication.
Defaults	N/A	
Command	Global configuration mode	

Mode		
Usage Guide	If the AAA Portal Web security service is enabled on the device, users must use AAA for Portal Web authentication negotiation. You must use the aaa authentication iportal command to configure a default or optional method list for Portal Web authentication.	
Configuration Examples	The following example defines an AAA Portal Web authentication method list named rds_web. First the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. <pre>FS(config)# aaa authentication iportal rds_web group radius local</pre>	
Related Commands	Command	
	Description	
	aaa new-model	Enables the AAA security service.
	login authentication	Applies the Login authentication method to the terminal lines.
	username	Defines a local user database.
Platform Description	N/A	

1.9 aaa authentication login

	Use this command to enable AAA Login authentication and configure the Login authentication method list. Use the no form of this command to delete the authentication method list.	
	aaa authentication login { default list-name } method1 [method2..]	
	no aaa authentication login { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for Login authentication.
	list-name	Name of the user authentication method list, which could be any character strings
	method	It must be one of the keywords: local , none , group and subs . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS and TACACS+ server groups are supported.

	subs	Uses the subs database for authentication.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the AAA Login authentication security service is enabled on the device, users must use AAA for Login authentication negotiation. You must use the aaa authentication login command to configure a default or optional method list for Login authentication. The next method can be used for authentication only when the current method does not work. You need to apply the configured Login authentication method to the terminal line which needs Login authentication. Otherwise, the configured Login authentication method is invalid.	
Configuration Examples	The following example defines an AAA Login authentication method list named list-1. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. <pre>FS(config)# aaa authentication login list-1 group radius local</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	login authentication	Applies the Login authentication method to the terminal lines.
	username	Defines a local user database.
Platform Description	N/A	

1.10 aaa authentication ppp

	Use this command to enable the AAA authentication for PPP user and configure the PPP user authentication method list. Use the no form of this command to delete the authentication method list.	
	aaa authentication ppp { default list-name } method1 [method2...]	
	no aaa authentication ppp { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for PPP user authentication.
	<i>list-name</i>	Name of the user authentication method list, which could be any character strings

	<i>method</i>	It must be one of the keywords: local , none group and subs . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS server group is supported.
	subs	Uses the subs database for authentication.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the AAA PPP security service is enabled on the device, users must use AAA authentication for PPP negotiation. You must use the aaa authentication ppp command to configure a default or optional method list for PPP user authentication. The next method can be used for authentication only when the current method does not work.	
Configuration Examples	The following example defines an AAA authentication method list named rds_ppp for PPP session. In the authentication method list, first the RADIUS security server is used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. <pre>FS(config)# aaa authentication ppp rds_ppp group radius local</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	ppp authentication	Associates a specific method list with the PPP user.
	username	Defines a local user database.
Platform Description	N/A	

1.11 aaa authentication sslvpn

	Use this command to enable AAA authentication for the SSL VPN user and configure the SSL VPN user authentication method list. Use the no form of this command to delete the authentication method list.	
	aaa authentication sslvpn { default list-name } method1 [method2...]	
	no aaa authentication sslvpn { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for SSL VPN user authentication.
	<i>list-name</i>	Name of SSL VPN user authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: local , none , subs and group . One method list can contain up to four methods.
	local	Use the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS server group is supported.
	subs	Uses the subs database for authentication.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the SSL VPN security service is enabled on the device, users must use the AAA authentication for SSL VPN negotiation. You must use the aaa authentication sslvpn command to configure a default or optional method list for user authentication. The next method can be used for authentication only when the current method does not work.	
Configuration	The following example defines an AAA authentication method list named rds_sslvpn for SSL VPN session. In the	

Examples	authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication.	
	FS(config)# aaa authentication sslvpn rds_sslvpn group radius local	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.12 aaa authentication web-auth

	Use this command to enable AAA second-generation Web authentication and configure the second-generation Web authentication method list in global configuration mode.	
	Use the no form of this command to delete the authentication method list.	
	aaa authentication web-auth { default list-name } method1 [method2...]	
	no aaa authentication web-auth { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined authentication method list is used as the default method for the second-generation Web authentication.
	<i>list-name</i>	Name of second-generation Web authentication method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: local , none , subs and group . One method list can contain up to four methods.
	local	Uses the local user name database for authentication.
	none	Does not perform authentication.
	group	Uses the server group for authentication. At present, the RADIUS server group is supported.
	subs	Uses the subs database for authentication.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	If the AAA second-generation Web security service is enabled on the device, users must use AAA for the second-generation Web authentication negotiation. You must use the aaa authentication web-auth command to configure a default or optional method list for user authentication. The next method can be used for authentication only when the current method does not work.	

Configuration Examples	The following example defines an AAA authentication method list named rds_web . In the authentication method list, the RADIUS security server is first used for authentication. If the RADIUS security server does not respond, the local user database is used for authentication. <pre>FS(config)# aaa authentication web-auth rds_web group radius none</pre>				
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

1.13 aaa authorization commands

	Use this command to authorize the command executed by the user who has logged in the NAS CLI. Use the no form of this command to restore the default setting.	
	aaa authorization commands <i>level</i> { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	
	no aaa authorization commands <i>level</i> { default <i>list-name</i> }	
Parameter	Parameter	Description
Description	<i>level</i>	Command level to be authorized in the range from 0 to 15
	default	When this parameter is used, the following defined method list is used as the default method for command authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords: none and group . One method list can contain up to four methods.
	none	Do not perform authorization.
	group	Uses the server group for authorization. At present, the TACACS+ server group is supported.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS supports authorization of the commands executed by the users. When the users input and attempt to execute a command, AAA sends this command to the security server. This command is to be executed if the security server allows to. Otherwise, it will prompt command deny. It is necessary to specify the command level when configuring the command authorization, and this specified command level is the default command level. The configured command authorization method must be applied to terminal line which requires the command authorization. Otherwise, the configured command authorization method is ineffective.	
Configuration	The following example uses the TACACS+ server to authorize the level 15 command.	

Examples	FS(config)# aaa authorization commands 15 default group tacacs+	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	authorization commands	Applies the command authorization for the terminal line.
Platform Description	N/A	

1.14 aaa authorization config-commands

	Use this command to authorize the configuration commands (including in the global configuration mode and its sub-mode). Use the no form of this command to restore the default setting.	
	aaa authorization config-commands	
	no aaa authorization config-commands	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	If you only authorize the commands in the non-configuration mode (for example, privileged EXEC mode), you can use the no form of this command to disable the authorization function in the configuration mode, and execute the commands in the configuration mode and its sub-mode without command authorization.	
Configuration Examples	The following example enables the configuration command authorization function. FS(config)# aaa authorization config-commands	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.
Platform Description	N/A	

1.15 aaa authorization console

	Use this command to authorize the commands of the users who have logged in the console. Use the no form of this command to restore the default setting.	
	aaa authorization console	

	no aaa authorization console	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS supports to identify the users logged in from the console and from other terminals, configure whether to authorize the users logged in from the console or not. If the command authorization function is disabled on the console, the authorization method list applied to the console line is ineffective.	
Configuration Examples	The following example enables the aaa authorization console function. <pre>FS(config)# aaa authorization console</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa authorization commands	Defines the AAA command authorization.
	authorization commands	Applies the command authorization to the terminal line.
Platform Description	N/A	

1.16 aaa authorization exec

	Use this command to authorize the users logged in the NAS CLI and assign the authority level. Use the no form of this command to restore the default setting.	
	aaa authorization exec { default list-name } method1 [method2...]	
	no aaa authorization exec { default list-name }	
Parameter	Parameter	Description
Description	default	When this parameter is used, the following defined method list is used as the default method for Exec authorization.
	<i>list-name</i>	Name of the user authorization method list, which could be any character strings
	<i>method</i>	It must be one of the keywords listed in the following table. One method list can contain up to four methods.
	local	Uses the local user name database for authorization.
	none	Does not perform authorization.
	group	Uses the server group for authorization. At present, the RADIUS server group is supported.

Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	FSOS supports authorization of users logged in the NAS CLI and assignment of CLI authority level (0-15). The aaa authorization exec function is effective on condition that Login authentication function has been enabled. It cannot enter the CLI if it fails to enable the aaa authorization exec. You must apply the exec authorization method to the terminal line; otherwise the configured method is ineffective.	
Configuration Examples	The following example uses the RADIUS server to authorize Exec. <pre>FS(config)# aaa authorization exec default group radius</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	authorization exec	Applies the command authorization to the terminal line.
	username	Defines a local user database.
Platform Description	N/A	

1.17 aaa authorization network

	Use this command to authorize the service requests (including such protocols as PPP and SLIP) from the users that access the network. Use the no form of this command to restore the default setting.	
	aaa authorization network { default list-name } method1 [method2...]	
	no aaa authorization network { default list-name }	
Parameter Description	Parameter	Description
	default	When this parameter is used, the following defined method list is used as the default method for Network authorization.
	<i>method</i>	It must be one of the keywords: none and group. One method list can contain up to four methods.
	none	Does not perform authorization.
	group	Uses the server group for authorization. At present, the RADIUS server group is supported.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	

Usage Guide	FSOS supports authorization of all the service requests related to the network, such as PPP and SLIP. If authorization is configured, all the authenticated users or interfaces will be authorized automatically. Three different authorization methods can be specified. Like authorization, the next method can be used for authorization only when the current authorization method does not work. If the current authorization method fails, other subsequent authorization method is not used. The RADIUS server authorizes authenticated users by returning a series of attributes. Therefore, RADIUS authorization is based on RADIUS authorization. RADIUS authorization is performed only when the user passes the RADIUS authorization.	
Configuration Examples	The following example uses the RADIUS server to authorize network services. FS(config)# aaa authorization network default group radius	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa accounting	Defines AAA accounting.
	aaa authentication	Defines AAA authentication.
	username	Defines a local user database.
Platform Description	N/A	

1.18 aaa domain

	Use this command to configure the domain attributes. Use the no form of this command to restore the default setting.	
	aaa domain { default domain-name }	
	no aaa domain { default domain-name }	
Parameter	Parameter	Description
Description	default	Uses this parameter to configure the default domain.
	domain-name	The name of the specified domain
Defaults	No domain is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to configure the domain-name-based AAA service. The default is to configure the default domain. That is the method list used by the network device if the users are without domain information. The <i>domain-name</i> is the specified domain name, if the users are with this <i>domain name</i> , the method lists associated with this domain are used. At present, the system can configure up to 32 domains.	
Configuration Examples	The following example configures the domain name. FS(config)# aaa domain FS.com	

	FS(config-aaa-domain)#	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.
Platform	N/A	
Description		

1.19 aaa domain enable

	Use this command to enable domain-name-based AAA service. Use the no form of this command to restore the default setting.	
	aaa domain enable	
	no aaa domain enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	To perform the domain-name-based AAA service configuration, enable this service.	
Configuration Examples	The following example enables the domain-name-based AAA service. FS(config)# aaa domain enable	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	show aaa doamain	Displays the domain configuration.
Platform	N/A	
Description		

1.20 aaa local authentication attempts

	Use this command to set login attempt times.	
	aaa local authentication attempts <i>max-attempts</i>	
Parameter	Parameter	Description
Description	<i>max-attempts</i>	In the range from 1 to 2,147,483,647

Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to configure login attempt times.	
Configuration Examples	The following example sets login attempt times to 6. FS #configure terminal FS(config)#aaa local authentication attempts 6	
Related Commands	Command	Description
	show running-config	Displays the current configuration of the switch.
	show aaa logout	Displays the logout configuration parameter of current login.
Platform Description	N/A	

1.21 aaa local authentication logout-time

	Use this command to configure the lockout-time period when the login user has attempted for more than the limited times.	
	aaa local authentication lockout-time <i>lockout-time</i>	
Parameter	Parameter	Description
Description	<i>lockout-time</i>	In the range from 1 to 3200 in the unit of minutes
Defaults	The default is 15 minutes.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to configure the length of lockout-time when the login user has attempted for more than the limited times.	
Configuration Examples	The following example sets the lockout-time period to 5 minutes. FS#configure terminal FS(config)#aaa local authentication lockout-time 5	
Related Commands	Command	Description
Commands	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.

Platform	N/A
Description	

1.22 aaa log enable

	Use this command to enable the system to print the syslog informing AAA authentication success. Use the no form of this command to restore the default setting.	
	aaa log enable	
	no aaa log enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable the system to print the syslog informing aaa authentication success.	
Configuration Examples	The following example disables the system to print the syslog informing aaa authentication success. FS(config)# no aaa log enable	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

1.23 aaa log rate-limit

	Use this command to set the rate of printing the syslog informing AAA authentication success. Use the no form of this command to restore the default printing rate.	
	aaa log rate-limit num	
	no aaa log rate-limit	
Parameter	Parameter	Description
Description	<i>num</i>	The number of syslog entries printed per second. The range is from 0 to 65,535. 0 indicates the printing rate is not limited.
Defaults	The default is 5.	
Command	Global configuration mode	

Mode		
Usage Guide	Too much printing may flood the screen or even reduce device performance. In this case, use this command to adjust the printing rate.	
Configuration Examples	The following example sets the rate of printing the syslog informing AAA authentication success to 10. FS(config)# aaa log rate-limit 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.24 aaa new-model

	Use this command to enable the FSOS AAA security service. Use the no form of this command to restore the default setting.	
	aaa new-model	
	no aaa new-model	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable AAA. If AAA is not enabled, none of the AAA commands can be configured.	
Configuration Examples	The following example enables the AAA security service. FS(config)# aaa new-model	
Related Commands	Command	Description
	aaa authentication	Defines a user authentication method list.
	aaa authorization	Defines a user authorization method list.
	aaa accounting	Defines a user accounting method list.
Platform Description	N/A	

1.25 access-limit

	Use this command to configure the number of users limit for the domain, which is only valid for the IEEE802.1 users. Use the no form of this command to restore the default setting.	
	access-limit <i>num</i>	
	no access-limit	
Parameter	Parameter	Description
Description	<i>num</i>	The number used for the user limitation is only valid for the IEEE802.1 users.
Defaults	By default, no number of users is limited.	
Command Mode	Domain configuration mode	
Usage Guide	This command limits the number of users for the domain.	
Configuration Examples	The following example sets the number of users to 20 for the domain named FS.com. <pre>FS(config)# aaa domain FS.com FS(config-aaa-domain)# access-limit 2</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Switchover the user level.
	show aaa domain	Defines a local user database.
Platform	N/A	
Description		

1.26 accounting network

	Use this command to configure the Network accounting list. Use the no form of this command to restore the default setting.	
	accounting network { default <i>list-name</i> }	
	no accounting network	
Parameter	Parameter	Description
Description	default	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the network accounting list
Defaults	With no method list specified, if the user sends the request, the device will attempt to specify the default method list for the user.	

Command Mode	Domain configuration mode	
Usage Guide	Use this command to configure the Network accounting method list for the specified domain.	
Configuration Examples	The following example sets the Network accounting method list for the specified domain. <pre>FS(config)# aaa domain FS.com FS(config-aaa-domain)# accounting network default</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.
Platform Description	N/A	

1.27 authentication dot1x

	Use this command to configure the IEEE802.1x authentication list. Use the no form of this command to restore the default setting.	
	authentication dot1x { default list-name }	
	no authentication dot1x	
Parameter Description	Parameter	Description
	default	Uses this parameter to specify the default method list
	<i>list-name</i>	The name of the specified method list
Defaults	With no method list specified, if users send the request, the device will attempt to specify the default method list for users.	
Command Mode	Domain configuration mode	
Usage Guide	Specify an IEEE802.1x authentication method list for the domain.	
Configuration Examples	The following example sets an IEEE802.1x authentication method list for the specified domain. <pre>FS(config)# aaa domain FS.com FS(config-aaa-domain)# authentication dot1x default</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.

Platform	N/A
Description	

1.28 authorization network

	Use this command to configure the Network authorization list. Use the no form of this command to restore the default setting.	
	authorization network { default list-name }	
	no authorization network	
Parameter	Parameter	Description
Description	default	Uses this parameter to specify the default method list.
	<i>list-name</i>	The name of the specified method list
Defaults	With no method list specified, if users send the request, the device will attempt to specify the default method list for users.	
Command Mode	Domain configuration mode	
Usage Guide	Specify an authorization method list for the domain.	
Configuration Examples	The following example sets an authorization method list for the specified domain. <pre>FS(config)# aaa domain FS.com FS(config-aaa-domain)# authorization network default</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain	Displays the domain configuration.
Platform	N/A	
Description		

1.29 clear aaa local user lockout

	Use this command to clear the lockout user list.	
	clear aaa local user lockout { all user-name word }	
Parameter	Parameter	Description
Description	all	Indicates all locked users.
	user-name word	Indicates the ID of the locked User.

Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear all the user lists or a specified user list.	
Configuration Examples	The following example clears the logout user list. FS(config)# clear aaa local user lockout all	
Related Commands	Command	Description
	show running-config	Displays the current configuration of the switch.
	show aaa lockout	Displays the lockout configuration parameter of current login.
Platform Description	N/A	

1.30 show aaa accounting update

	Use this command to display the accounting update information.	
	show aaa accounting update	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the accounting update interval and whether the accounting update is enabled.	
Configuration Examples	The following example displays the accounting update information. FS# show aaa accounting update	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
Platform Description	N/A	

1.31 show aaa domain

	Use this command to display all current domain information.	
	show aaa domain [default <i>domain-name</i>]	
Parameter	Parameter	Description
Description	default	Displays the default domain.
	<i>domain-name</i>	Displays the specified domain.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	If no domain-name is specified, all domain information will be displayed.	
Configuration Examples	The following example displays the domain named domain.com. <pre>FS(config)# show aaa domain domain.com =====Domain domain.com===== State: Active Username format: Without-domain Access limit: No limit 802.1X Access statistic: 0 Selected method list: authentication dot1x default</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
Platform Description	N/A	

1.32 show aaa logout

	Use this command to display the logout configuration.	
	show aaa logout	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the lockout configuration.	
Configuration Examples	The following example displays the lockout configuration. FS# show aaa lockout Lock tries: 3 Lock timeout: 15 minutes	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.33 show aaa group

	Use this command to display all the server groups configured for AAA.																			
	show aaa group																			
Parameter	Parameter	Description																		
Description	N/A	N/A																		
Defaults	N/A																			
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																			
Usage Guide	N/A																			
Configuration Examples	The following command displays all the server groups. <pre>FS# show aaa group</pre> <table><thead><tr><th>Type</th><th>Reference</th><th>Name</th></tr></thead><tbody><tr><td>radius</td><td>1</td><td>radius</td></tr><tr><td>tacacs+</td><td>1</td><td>tacacs+</td></tr><tr><td>radius</td><td>1</td><td>dot1x_group</td></tr><tr><td>radius</td><td>1</td><td>login_group</td></tr><tr><td>radius</td><td>1</td><td>enable_group</td></tr></tbody></table>		Type	Reference	Name	radius	1	radius	tacacs+	1	tacacs+	radius	1	dot1x_group	radius	1	login_group	radius	1	enable_group
Type	Reference	Name																		
radius	1	radius																		
tacacs+	1	tacacs+																		
radius	1	dot1x_group																		
radius	1	login_group																		
radius	1	enable_group																		
Related Commands	Command	Description																		
	aaa group server	Configures the AAA server group.																		

Platform	N/A
Description	

1.34 show aaa method-list

	Use this command to display all AAA method lists.	
	show aaa method-list	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display all AAA method lists.	
Configuration Examples	The following example displays the AAA method list. <pre> FS# show aaa method-list Authentication method-list aaa authentication login default group radius aaa authentication ppp default group radius aaa authentication dot1x default group radius aaa authentication dot1x san-f local group angel group rain none aaa authentication enable default group radius Accounting method-list aaa accounting network default start-stop group radius Authorization method-list aaa authorization network default group radius </pre>	
Related Commands	Command	Description
	aaa authentication	Defines a user authentication method list
	aaa authorization	Defines a user authorization method list
	aaa accounting	Defines a user accounting method list
Platform	N/A	
Description		

1.35 show aaa user

	Use this command to display AAA user information.
	show aaa user { all logout by-id session-id by-name user-name }

Parameter	Parameter	Description
Description	all	Displays all AAA user information.
	lockout	Displays the locked AAA user information.
	by-id <i>session-id</i>	Displays the information of the AAA user that with a specified session ID.
	by-name <i>user-name</i>	Displays the information of the AAA user with a specified user name.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display AAA user information.	
Configuration Examples	The following example displays AAA user information. <pre> FS#show aaa user all ----- Id ---- Name 2345687901 wwxy ----- FS# show aaa user by-id 2345687901 ----- Id ---- Name 2345687901 wwxy FS# show aaa user by-name wwxy ----- Id ---- Name 2345687901 wwxy ----- FS# show aaa user lockout Name Tries Lock Timeout(min) ----- FS# </pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

1.36 state

	Use this command to set whether the configured domain is valid. Use the no form of this command to restore the default setting.	
	state { block active }	
	no state	
Parameter Description	Parameter	Description
	block	The configured domain is invalid.
	active	The configured domain is valid.
Defaults	The default is active.	
Command Mode	Domain configuration mode	
Usage Guide	Use this command to set whether the specified configured domain is valid.	
Configuration Examples	The following example sets the configured domain to be invalid. <pre>FS(config)# aaa domain FS.com FS(config-aaa-domain)# state block</pre>	
Related Commands	Command	Description
	aaa new-model	Enables the AAA security service.
	aaa domain enable	Enables the domain-name-based AAA service.
	show aaa domain enable	Displays the domain configuration.
Platform Description	N/A	

2 RADIUS Commands

2.1 aaa group server radius

	Use this command to enter AAA server group configuration mode. Use the no form of this command to restore the default setting.	
	aaa group server radius <i>name</i>	
	no aaa group server radius <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Server group name. Keywords “radius” and “tacacs +” are excluded as they are the default RADIUS and TACACS+ server group names.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure a RADIUS AAA server group.	
Configuration Examples	The following example configures a RADIUS AAA server group named ss. <pre> FS(config)# aaa group server radius ss FS(config-gs-radius)# end FS# show aaa group Type Reference Name ----- radius 1 radius tacacs+ 1 tacacs+ radius 1 ss </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.2 ip radius source-interface

	Use this command to specify the source IP address for the RADIUS packet. Use the no form of this command to delete the source IP address for the RADIUS packet.
	ip radius source-interface <i>interface-name</i>
	no radius source-interface <i>interface-name</i>

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface that the source IP address of the RADIUS packet belongs to.
Defaults	The source IP address of the RADIUS packet is set by the network layer.	
Command mode	Global configuration mode	
Usage Guide	In order to reduce the NAS information to be maintained on the RADIUS server, use this command to set the source IP address of the RADIUS packet. This command uses the first IP address of the specified interface as the source IP address of the RADIUS packet. This command is used in the layer 3 devices.	
Configuration Examples	The following example specifies that the RADIUS packet obtains an IP address from the fastEthernet 0/0 interface and uses it as the source IP address of the RADIUS packet. FS(config)# ip radius source-interface fastEthernet 0/0	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS server.
	ip address	Configures the IP address of the interface.
Platform Description	N/A	

2.3 ip oob

	Use this command to specify the MGMT port used in the TACACS+ server group. Use the no form of this command to restore the default setting.	
	ip oob [<i>via mgmt_name</i>]	
	no ip oob	
Parameter Description	Parameter	Description
	<i>mgmt_name</i>	MGMT port name
Defaults	N/A	
Command Mode	TACACS+ server group configuration mode	
Usage Guide	Use the aaa group server tacacs+ command to enter TACACS+ server group configuration mode. If no port is specified as the MGMT port. MGMT Port 0 is default.	

Configuration Examples		
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.4 ip vrf forwarding

	Use this command to select a VRF for the AAA server group. Use the no form of this command to restore the default setting.	
	ip vrf forwarding <i>vrf_name</i>	
	no ip vrf forwarding	
Parameter Description	Parameter	Description
	<i>vrf_name</i>	VRF name
Defaults	N/A	
Command Mode	Server group configuration mode	
Usage Guide	This command is used to select a VRF for the specified server.	
Configuration Examples	The following example selects the VRF named <i>vrf_name</i> for AAA server group <i>ss</i> . <pre> FS(config)# aaa group server radius ss FS(config-gs-radius)# server 192.168.4.12 FS(config-gs-radius)# server 192.168.4.13 FS(config-gs-radius)# ip vrf forwarding vrf_name FS(config-gs-radius)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.5 radius vendor-specific extend

	Use this command to extend RADIUS not to differentiate the IDs of private vendors. Use the no form of this command to restore the default setting.	
	radius vendor-specific extend	
	no radius vendor-specific extend	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Only the private vendor IDs of FS are recognized.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to identify the attributes of all vendor IDs by type.	
Configuration Examples	The following example extends RADIUS so as not to differentiate the IDs of private vendors: <pre>FS(config)# radius vendor-specific extend</pre>	
Related Commands	Command	Description
	radius attribute	Configures vendor type.
	radius set qos cos	Sets the QoS value sent by the RADIUS server as the cos value of the interface.
Platform Description	N/A	

2.6 radius vendor-specific attribute support

	Use this command to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor. Use the no form of this command to configure that RADIUS accounting request packets do not carry the private attribute of a specified vendor.	
	radius vendor-specific attribute support { cisco huawei ms}	
	no radius vendor-specific attribute support { cisco huawei ms}	
Parameter Description	Parameter	Description
	cisco	Indicates the private attribute of Cisco.
	huawei	Indicates the private attribute of Huawei.
	ms	Indicates the private attribute of Microsoft.

Defaults	By default, RADIUS accounting request packets carry the private attribute of a specified vendor.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure whether RADIUS accounting request packets carry the private attribute of a specified vendor as required.	
Configuration Examples	1. The following example configures that RADIUS accounting request packets carry the private attribute of Huawei. <pre>FS(config)# radius vendor-specific attribute support huawei</pre>	
	2. The following example configures that RADIUS accounting request packets do not carry the private attribute of Huawei. <pre>FS(config)# no radius vendor-specific attribute support huawei</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.7 radius-server account update retransmit

	Use this command to configure accounting update packet retransmission for the second generation Web authentication user. Use the no form of this command to restore the default setting,	
	radius-server account update retransmit	
	no radius-server account update retransmit	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to configure accounting update packet retransmission for the second generation Web authentication user exclusively.	

Configuration Examples	The following example configures accounting update packet retransmission for the second generation Web authentication user. FS(config)#radius-server account update retransmit	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.8 radius-server attribute 31

	Use this command to specify the MAC-based format of RADIUS Calling-Station-ID attribute. Use the no form of this command to restore the default setting.	
	radius-server attribute 31 mac format { ietf normal unformatted }	
	no radius-server attribute 31 mac format	
Parameter Description	Parameter	Description
	ietf	The standard format specified by the IETF RFC3580. '-'is used as the separator, for example: 00-D0-F8-33-22-AC.
	normal	Normal format representing the MAC address. ;'is used as the separator. For example: 00d0.f833.22ac.
	unformatted	No format and separator. By default, unformatted is used. For example: 00d0f83322ac.
Defaults	The default format is unformatted.	
Command Mode	Global configuration mode	
Usage Guide	Some RADIUS security servers (mainly used to 802.1x authentication) may identify the IETF format only. In this case, the RADIUS Calling-Station-ID attribute shall be set as the IETF format type.	
Configuration Examples	The following example defines the RADIUS Calling-Station-ID attribute as IETF format. FS(config)# radius-server attribute 31 mac format ietf	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS server.
Platform Description	N/A	

2.9 radius-server attribute class

	Use this command to analyze the flow control value of the RADIUS CLASS attributes. Use the no form of this command to restore the default setting.	
	radius-server attribute class user-flow-control { format-16bytes format-32bytes }	
	no radius-server attribute class user-flow-control	
Parameter Description	Parameter	Description
	user-flow-control	Analyzes flow control value in the CLASS attribute.
	format-16bytes	Sets the format of flow control value to 16 bytes.
	format-32bytes	Sets the format of flow control value to 32 bytes.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is required if the server pushes the flow control value through the CLASS attribute.	
Configuration Examples	The following example analyzes the flow control value of the CLASS attribute and sets the format to 32 bytes. FS(config)#radius-server attribute class user-flow-control format-32bytes	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.10 radius-server dead-criteria

	Use this command to configure criteria on a device to determine that the Radius server is unreachable. Use the no form of this command to restore the default setting.	
	radius-server dead-criteria { time seconds [tries number] tries number }	
	no radius-server dead-criteria { time [tries] tries }	
Parameter Description	Parameter	Description
	time seconds	Configures the timeout value. If the device does not receive a correct response packet from the Radius server within the specified time, the Radius server is considered to be unreachable. The value is in the range from 1 to 120 in the unit of seconds.
	tries number	Configures the successive timeout times. When sending a request from the

		device to the Radius server times out for the specified times, the device considers that the Radius server is unreachable. The value is in the range from 1 to 100 in the unit of seconds.
Defaults	The default time seconds is 60 and tries number is 10.	
Command Mode	Global configuration mode	
Usage Guide	If a Radius server meets the timeout and timeout times at the same time, it is considered to be unreachable. This command is used to adjust the parameter conditions of timeout and timeout times.	
Configuration Examples	The following example sets the timeout to 120 seconds and timeout times to 20. <pre>FS(config)# radius-server dead-criteria time 120 tries 20</pre>	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server deadtime	Defines the duration when a device stops sending any requests to an unreachable Radius server.
	radius-server timeout	Defines the timeout for the packet re-transmission.
Platform Description	N/A	

2.11 radius-server deadtime

	Use this command to configure the duration when a device stops sending any requests to an unreachable Radius server. Use the no form of this command to restore the default setting.	
	radius-server deadtime minutes	
	no radius-server deadtime	
Parameter Description	Parameter	Description
	<i>minutes</i>	Defines the duration in minutes when the device stops sending any requests to the unreachable Radius server. The value is in the range from 1 to 1,440 in the unit of minutes.
Defaults	The default value of <i>minutes</i> is 0, that is, the device keeps sending requests to the unreachable Radius server.	
Command Mode	Global configuration mode	

Usage Guide	If active Radius server detection is enabled on the device, the time parameter of this command does not take effect on the Radius server. Otherwise, the Radius server becomes reachable when the duration set by this command is shorter than the unreachable time.	
Configuration Examples	The following example sets the duration when the device stops sending requests to 1 minute. FS(config)# radius-server deadtime 1	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server dead-criteria	Defines the criteria to determine that a Radius server is unreachable.
Platform Description	N/A	

2.12 radius-server host

	Use this command to specify a RADIUS security server host. Use the no form of this command to restore the default setting.	
	radius-server host [oob [via <i>mgmt-name</i>]] { <i>ipv4-address</i> <i>ipv6-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [test username <i>name</i> [idle-time <i>time</i>] [ignore-auth-port] [ignore-acct-port]] [key [0 7] <i>text-string</i>]	
	no radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	oob [<i>via mgmt-name</i>]	Specifies an MGMT port as the source port for TACACS+ communication. The default is MGMT Port 0.
	<i>ipv4-address</i>	IPv6 address of the RADIUS security server host.
	<i>ipv6-address</i>	IPv4 address of the RADIUS security server host.
	auth-port	UDP port used for RADIUS authentication.
	<i>port-number</i>	Number of the UDP port used for RADIUS authentication. If it is set to 0, this host does not perform authentication.
	acct-port	UDP port used for RADIUS accounting.
	<i>port-number</i>	Number of the UDP port used for RADIUS accounting. If it is set to 0, this host does not perform accounting.
	test username <i>name</i>	(Optional) Enables the active detection to the RADIUS security server and specify the username used by the active detection.
	idle-time <i>time</i>	(Optional) Sets the interval of sending the test packets to the reachable RADIUS security server, which is 60 minutes by default and in the range of 1 to 1440 minutes (namely 24 hours).
	ignore-auth-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.

	ignore-acct-port	(Optional) Disables the detection to the authentication port on the RADIUS security server. It is enabled by default.
	key [0 7] <i>text-string</i>	Configure a shared key for the server. The type of encryption can be specified. 0 is no encryption and 7 is simple encryption. The default is 0.
Defaults	No RADIUS host is specified by default.	
Command Mode	Global configuration mode	
Usage Guide	In order to implement the AAA security service using RADIUS, you must define a RADIUS security server. You can define one or more RADIUS security servers using the radius-server host command.	
Configuration Examples	The following example defines a RADIUS security server host: <pre>FS(config)# radius-server host 192.168.12.1</pre> The following example defines a RADIUS security server host in the IPv4 environment, enable the active detection with the detection interval 60 minutes and disable the accounting UDP port detection: <pre>FS(config)# radius-server host 192.168.100.1 test username viven idle-time 60 ignore-acct-port</pre> The following example defines a RADIUS security server host in the IPv6 environment <pre>FS(config)# radius-server host 3000::100</pre>	
Related Commands	Command	Description
	aaa authentication	Defines the AAA authentication method list
	radius-server key	Defines a shared password for the RADIUS security server.
	radius-server retransmit	Defines the number of RADIUS packet retransmissions.
Platform Description	N/A	

2.13 radius-server key

	Use this command to define a shared password for the network access server (device) to communicate with the RADIUS security server. Use the no form of this command to restore the default setting.
	radius-server key [0 7] <i>text-string</i>
	no radius-server key

Parameter Description	Parameter	Description
	<i>text-string</i>	Text of the shared password
	0 7	Password encryption type. 0: no encryption; 7: Simply-encrypted.
Defaults	No shared password is specified by default.	
Command Mode	Global configuration mode.	
Usage Guide	A shared password is the basis for communications between the device and the RADIUS security server. In order to allow the device to communicate with the RADIUS security server, you must define the same shared password on the device and the RADIUS security server.	
Configuration Examples	The following example defines the shared password aaa for the RADIUS security server: <pre>FS(config)# radius-server key aaa</pre>	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server retransmit	Defines the number of RADIUS packet retransmissions.
	radius-server timeout	Defines the timeout for the RADIUS packet.
Platform Description	N/A	

2.14 radius-server retransmit

	Use this command to configure the number of packet retransmissions before the device considers that the RADIUS security server does not respond. Use the no form of this command to restore the default setting.	
	radius-server retransmit <i>retries</i>	
	no radius-server retransmit	
Parameter Description	Parameter	Description
	<i>retries</i>	Number of retransmissions in the range from 0 to 100. The value of 0 indicates no retransmission.
Defaults	The default is 3.	

Command Mode	Global configuration mode.	
Usage Guide	AAA uses the next method to authenticate users only when the current security server for authentication does not respond. When the device retransmits the RADIUS packet for the specified times and the interval between every two retries is timeout, the device considers that the security sever does not respond.	
Configuration Examples	The following example sets the number of retransmissions to 4. FS(config)# radius-server retransmit 4	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server key	Defines a shared password for the RADIUS server.
	radius-server timeout	Defines the timeout for the RADIUS packet.
Platform Description	N/A	

2.15 radius-server source-port

	Use this command to configure the source port to send RADIUS packets. Use the no form of this command to restore the default setting.	
	radius-server source-port <i>port</i>	
	no radius-server source-port	
Parameter Description	Parameter	Description
	<i>port</i>	The port ID, in the range from 0 to 65535.
Defaults	The default is a random number.	
Command Mode	Global configuration mode	
Usage Guide	The source port is random by default. This command is used to specify a source port.	
Configuration Examples	The following example configures source port 10000 to send RADIUS packets. FS(config)# radius-server source-port 10000	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

2.16 radius-server timeout

	Use this command to set the time for the device to wait for a response from the security server after retransmitting the RADIUS packet. Use the no form of this command to restore the default setting.	
	radius-server timeout <i>seconds</i>	
	no radius-server timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout in the range from 1 to 1,000 in the unit of seconds.
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to change the timeout of packet retransmission.	
Configuration Examples	The following example sets the timeout to 10 seconds. <pre>FS(config)# radius-server timeout 10</pre>	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server retransmit	Defines the number of the RADIUS packet retransmissions.
	radius-server key	Defines a shared password for the RADIUS server.
Platform	N/A	
Description		

2.17 radius-server authentication attribute

	Use this command to enable access-request packets to contain a specified RADIUS attribute. Use the no or default form of this command to restore the default setting.
	radius-server authentication attribute <i>type package</i>
	no radius-server authentication attribute <i>type package</i>
	default radius-server authentication attribute <i>type package</i>
	Use this command to disable access-request packets to contain a specified RADIUS attribute. Use the no or default form of this command to restore the default setting.

	radius-server authentication attribute <i>type</i> unpackage	
	no radius-server authentication attribute <i>type</i> unpackage	
	default radius-server authentication attribute <i>type</i> unpackage	
Parameter Description	Parameter	Description
	<i>type</i>	RADIUS attribute in the range from 1 to 255
Defaults	RFC-compliant	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable access-request packets to contain a specified RADIUS attribute.	
Configuration Examples	The following example disables access-request packets to contain attribute NAS-PORT-ID. <pre>FS(config)# radius-server authentication attribute 87 unpackage</pre>	
Platform Description	N/A	

2.18 radius-server account attribute

	Use this command to enable account-request packets to contain a specified RADIUS attribute. Use the no or default form of this command to restore the default setting. radius-server account attribute <i>type</i> package	
	no radius-server account attribute <i>type</i> package	
	default radius-server account attribute <i>type</i> package	
	Use this command to disable account-request packets to contain a specified RADIUS attribute. Use the no or default form of this command to restore the default setting.	
	radius-server account attribute <i>type</i> unpackage no radius-server account attribute <i>type</i> unpackage	
	default radius-server account attribute <i>type</i> unpackage	
Parameter Description	Parameter	Description
	<i>type</i>	RADIUS attribute in the range from 1 to 255
Defaults	RFC-compliant	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable or disable account-request packets to contain a specified RADIUS attribute.	

Configuration	The following example disables account-request packets to contain attribute NAS-PORT-ID.
Examples	FS(config)# radius-server account attribute 87 unpackage
Platform	
Description	N/A

2.19 radius-server authentication vendor

	Use this command to enable access-request packets to contain vendor-specific RADIUS attributes. Use the no or default form of this command to restore the default setting. radius-server authentication vendor [cmcc microsoft cisco] package	
	no radius-server authentication vendor <i>vendor_name</i> package default radius-server authentication vendor <i>vendor_name</i> package	
Parameter	Parameter	Description
Description	cmcc microsoft cisco	Vendor name
Defaults	Access-request packets do not contain vendor- specific RADIUS attributes by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable access-request packets to contain vendor- specific RADIUS attributes.	
Configuration	The following example enables access-request packets to contain "cmcc".	
Examples	FS(config)# radius-server authentication vendor cmcc package	
Platform	N/A	
Description		

2.20 radius-server account vendor

	Use this command to enable account-request packets to contain vendor-specific RADIUS attributes. Use the no or default form of this command to restore the default setting.	
	radius-server account vendor [cmcc microsoft cisco] package	
	no radius-server account vendor <i>vendor_name</i> package default radius-server account vendor <i>vendor_name</i> package	
Parameter	Parameter	Description
Description	cmcc microsoft cisco	Vender name
Defaults	Account-request packets do not contain vendor- specific RADIUS attributes by default.	

Command Mode	Global configuration mode
Usage Guide	Use this command to enable account-request packets to contain vendor-specific RADIUS attributes.
Configuration Examples	The following example enables account-request packets to contain "cmcc". FS(config)# radius-server account vendor cmcc package
Platform Description	N/A

2.21 radius set qos cos

	Use this command to set the QoS value sent by the RADIUS server as the CoS value of the interface. Use the no form of this command to restore the default setting.	
	radius set qos cos	
	no radius set qos cos	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Set the QoS value sent by the RADIUS server as the DSCP value.	
Command Mode	Global configuration mode.	
Usage Guide	This command is used to set the QoS value sent by the RADIUS server as the CoS value, and the DSCP value by default.	
Configuration Examples	The following example sets the QoS value sent by the RADIUS server as the CoS value of the interface: FS(config)# radius set qos cos	
Related Commands	Command	Description
	radius vendor-specific extend	Extends RADIUS as not to differentiate the IDs of private vendors.
Platform Description	N/A	

2.22 radius support cui

	Use this command to enable RADIUS to support the cui function. Use the no form of this command to restore the default setting.

	radius support cui	
	no radius support cui	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to enable RADIUS to support the cui function.	
Configuration Examples	The following example enables RADIUS to support the cui function. FS(config)# radius support cui	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.23 server auth-port acct-port

	Use this command to add the server of the AAA server group. Use the no form of this command to restore the default setting.	
	server { <i>ipv4-addr</i> <i>ipv6-addr</i> } [auth-port <i>port1</i>] [acct-port <i>port2</i>]	
	no server { <i>ipv4-addr</i> <i>ipv6-addr</i> } [auth-port <i>port1</i>] [acct-port <i>port2</i>]	
Parameter Description	Parameter	Description
	<i>ip-addr</i>	Server IP address
	<i>ipv6-addr</i>	Server IPv6 address
	<i>port1</i>	Server authentication port
	<i>port2</i>	Server accounting port
Defaults	No server is configured by default.	
Command Mode	Server group configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example adds server 192.168.4.12 to server group ss and sets the accounting port and authentication port to 5 and 6 respectively. <pre> FS(config)# aaa group server radius ss FS(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6 FS(config-gs-radius)# end FS# show aaa group Type Reference Name ----- radius 1 radius tacacs+ 1 tacacs+ radius 1 ss </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.24 show radius acct statistics

	Use this command to display RADIUS accounting statistics.	
	show radius acct statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays RADIUS accounting statistics. <pre> FS#show radius acct statistics Accounting Servers: Server Index..... 1 Server Address..... 192.168.1.1 Server Port..... 1813 Msg Round Trip Time..... 0 (msec) </pre>	

	First Requests..... 1 Retry Requests..... 1 Accounting Responses..... 0 Malformed Msgs..... 0 Bad Authenticator Msgs..... 0 Pending Requests.....	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.25 show radius auth statistics

	Use this command to display RADIUS authentication statistics.	
	show radius auth statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays RADIUS authentication statistics. <pre> FS#show radius auth statistics Authentication Servers: Server Index..... 1 Server Address..... 192.168.1.1 Server Port..... 1812 Msg Round Trip Time..... 0 (msec) First Requests..... 0 Retry Requests..... 0 Accept Responses..... 0 Reject Responses..... 0 Challenge Responses..... 0 Malformed Msgs..... 0 </pre>	

	Bad Authenticator Msgs..... 0 Pending Requests..... 0 Timeout Requests..... 0 Unknown type Msgs..... 0 Other Drops..... 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.26 show radius group

	Use this command to display RADIUS server group configuration.	
	show radius group	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays RADIUS server group configuration. <pre> FS#show radius group =====Radius group radius===== Vrf:not-set Server:192.168.1.1 Server key:FS Authentication port:1812 Accounting port:1813 State:Active </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

2.27 show radius parameter

	Use this command to display global RADIUS server parameters.	
	show radius parameter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays global RADIUS server parameters. <pre>FS# show radius parameter Server Timeout: 5 Seconds Server Deadtime: 0 Minutes Server Retries: 3 Server Dead Criteria: Time: 10 Seconds Tries: 10</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

2.28 show radius server

	Use this command to display the configuration of the RADIUS server.	
	show radius server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	

Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration of the RADIUS server. <pre> FS# show radius server Server IP: 192.168.4.12 Accounting Port: 23 Authen Port: 77 Test Username: viven Test Idle Time: 10 Minutes Test Ports: Authen Server State: Active Current duration 765s, previous duration 0s Dead: total time 0s, count 0 Statistics: Authen: request 15, timeouts 1 Author: request 0, timeouts 0 Account: request 0, timeouts 0 Server IP: 192.168.4.13 Accounting Port: 45 Authen Port: 74 Test Username: <Not Configured> Test Idle Time: 60 Minutes Test Ports: Authen and Accounting Server State: Active Current duration 765s, previous duration 0s Dead: total time 0s, count 0 Statistics: Authen: request 0, timeouts 0 Author: request 0, timeouts 0 Account: request 20, timeouts 0 </pre>	
Related Commands	Command	Description
	radius-server host	Defines the RADIUS security server.
	radius-server retransmit	Defines the number of RADIUS packet retransmissions.
	radius-server key	Defines a shared password for the RADIUS server.
	radius-server timeout	Defines the packet transmission timeout.
Platform	N/A	

Description	

2.29 show radius vendor-specific

	Use this command to display the configuration of the private vendors.	
	show radius vendor-specific	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration of the private vendors. <pre> FS#show radius vendor-specific id vendor-specific type-value ----- 1 max-down-rate 1 2 port-priority 2 3 user-ip 3 4 vlan-id 4 5 last-supPLICANT-vers 5 ion 6 net-ip 6 7 user-name 7 8 password 8 9 file-directory 9 10 file-count 10 11 file-name-0 11 12 file-name-1 12 13 file-name-2 13 14 file-name-3 14 15 file-name-4 15 16 max-up-rate 16 17 current-supPLICANT-version 17 18 flux-max-high32 18 19 flux-max-low32 19 20 proxy-avoid 20 21 dialup-avoid 21 </pre>	

	22	ip-privilege	22
	23	login-privilege	42
	26	ipv6-multicast-addre	79
		ss	
	27	ipv4-multicast-addre	87
		ss	
Related Commands	Command		Description
	radius-server host		Defines the RADIUS security server.
	radius-server retransmit		Defines the number of RADIUS packet retransmissions.
	radius-server key		Defines a shared password for the RADIUS server.
	radius-server timeout		Defines the packet transmission timeout.
Platform Description	N/A		

2.30 show radius attribute

	Use this command to display standard Radius attributes. show radius attribute	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Global configuration mode/Privileged EXEC mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays standard RADIUS attributes. <pre>FS#sh radius attribute type implicate ----- 1.....User-Name 2.....User-Password 3.....Chap-Password 4.....NAS-Ip-Addr 5.....Nas-Ip-Port 6.....Service-Type 7.....Framed-Protocol 8.....Frame-Ip-Address 9.....Framed-Ip-Mask</pre>	

10.....Framed-Routing
 11.....Filter-Id
 12.....Framed-Mtu
 13.....Framed-Compress
 14.....Login-Ip-Host
 15.....Login-Service
 16.....Login-Tcp-Port
 18.....Reply-Message
 19.....Callback-Num
 20.....Callback-Id
 22.....Framed-Route
 23.....Framed-IPX-Network
 24.....State
 25.....Class
 26.....Vendor-Specific
 27.....Session-Timeout
 28.....Idle-Timeout
 29.....Termination-Action
 30.....Called-Station-Id
 31.....Calling-Station-Id
 32.....Nas-Id
 33.....Proxy-State
 34.....Login-LAT-Service
 35.....Login-LAT-Node
 36.....Login-LAT-Group
 37.....Framed-AppleTalk-Link
 38.....Framed-AppleTalk-Net
 39.....Framed-AppleTalk-Zone
 40.....Acct-Status-Type
 41.....Acct-Delay-Time
 42.....Acct-Input-Octets
 43.....Acct-Output-Octets
 44.....Acct-Session-Id
 45.....Acct-Authentic
 46.....Acct-Session-Time
 47.....Acct-Input-Packet
 48.....Acct-Output-Packet
 49.....Acct-Terminate-Cause
 50.....Acct-Multi-Session-ID
 51.....Acct-Link-Count
 52.....Acct-Input-Gigawords
 53.....Acct-Output-Gigawords
 60.....Chap-Challenge
 61.....Nas-Port-Type

	62.....Port-Limit 63.....Login-Lat-Port 64.....Tunnel-Type 65.....Tunnel-Medium-Type 66.....Tunnel-Client-EndPoint 67.....Tunnel-Service-EndPoint 79.....eap msg 80.....Message-Authenticator 81.....group id 85.....Acct-Interim-Interval 87.....Nas-Port-Id 89.....cui 95.....Nas-Ipv6-Addr 96.....Framed-Interface-Id 97.....Framed-Ipv6-Prefix 98.....Login-Ipv6-Host 99.....Framed-Ipv6-Route 100.....Framed-Ipv6-Pool 168.....Framed-Ipv6-Addr
Platform Description	N/A

3 TACACS+ Commands

3.1 aaa group server tacacs+

	Use this command to configure different groups of TACACS+ server hosts. Use the no form of this command to remove a specified TACACS server group.	
	aaa group server tacacs+ group_name	
	no aaa group server tacacs+ group_name	
Parameter Description	Parameter	Description
	<i>group_name</i>	TACACS+ server group name, which cannot be radius or tacacs+ . The two names are the built-in group name.
Defaults	No TACACS+ server group is configured.	
Command Mode	Global configuration mode	
Usage Guide	After you group different TACACS+ servers, the tasks of authentication, authorization and accounting can be implemented by different server groups.	
Configuration Examples	The following example configures a TACACS+ server group named tac1, and configures a TACACS+ server with IP address 1.1.1.1 in this group: <pre>FS(config)#aaa group server tacacs+ tac1 FS(config-gs-tacacs+)# server 1.1.1.1</pre>	
Related Commands	Command	Description
	server	Configures server list of TACACS+ server group.
	ip vrf forwarding	Configures VRF name supported by TACACS+ server group.
Platform Description	N/A	

3.2 ip tacacs source-interface

	Use this command to use the IP address of a specified interface for all outgoing TACACS+ packets. Use the no form of this command to disable use of the specified interface IP address.
	ip tacacs source-interface interface-name
	no ip tacacs source-interface interface-name

Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface for the outgoing TACACS+ packets
Defaults	The source IP address of TACACS+ packets is set on the network layer.	
Command Mode	Global configuration mode	
Usage Guide	To decrease the work of maintaining massive NAS messages in TACACS+ server, use this command to use the IP address of a specified interface for all outgoing TACACS+ packets. This command specifies the primary IP address of the specified interface as the source address of TACACS+ packets on Layer 3 devices. If the specified interface is in a VRF instance, the route of this VRF instance is used for packet transmission.	
Configuration Examples	The following example specifies the IP address of GigabitEthernet 0/0 for the outgoing TACACS+ packets. <pre>FS(config)# ip tacacs source-interface gigabitEthernet 0/0</pre>	
Related Commands	Command	Description
	tacacs-server host	Defines a TACACS+ server.
	ip address	Configures the IP address of an interface.
Platform Description	N/A	

3.3 ip oob

	Use this command to specify the MGMT port used in the TACACS+ server group. Use the no form of this command to restore the default setting.	
	ip oob [<i>via mgmt_name</i>]	
	no ip oob	
Parameter Description	Parameter	Description
	<i>mgmt_name</i>	MGMT port name
Defaults	N/A	
Command Mode	TACACS+ server group configuration mode	
Usage Guide	Use the aaa group server tacacs+ command to enter TACACS+ server group configuration mode. No MGMT port is specified by default.	

Configuration Examples	N/A
Platform Description	N/A

3.4 ip vrf forwarding

	Use this command to configure the VRF used in the TACACS+ server group. Use the no form of this command to remove the VRF configuration from the TACACS+ server group.	
	ip vrf forwarding <i>vrf-name</i>	
	no ip vrf forwarding	
Parameter Description	Parameter	Description
	<i>vrf-name</i>	VRF name
Defaults	N/A	
Command Mode	TACACS+ server group configuration mode	
Usage Guide	Before you configure this command, you need to use the aaa group server tacacs+ command to enter TACACS+ server group configuration mode. The VRF instance must exist and be configured with a correct VRF name through the vrf definition command.	
Configuration Examples	The following example specifies the VRF instance named vpn1 for the TACACS+ server group: <pre>FS(config)# aaa group server tacacs+ tac1 FS(config-gs-tacacs+)# server 1.1.1.1 FS(config-gs-tacacs+)# ip vrf forwarding vpn1</pre>	
Related Commands	Command	Description
	aaa group server tacacs+	Configures the TACACS+ server group.
	server	Configures a server list of TACACS+ server group.
Platform Description	N/A	

3.5 server

	Use this command to configure the IP address of the TACACS+ server for the group server. Use the no form of this command to remove the TACACS+ server.
	server { <i>ipv4-address</i> <i>ipv6-address</i> }

	no server { <i>ipv4-address</i> <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	<i>ipv4-address</i>	IPv4 address of the TACACS+ server
	<i>ipv6-address</i>	IPv6 address of the TACACS+ server
Defaults	No TACACS+ server is configured by default.	
Command Mode	TACACS+ server group configuration mode	
Usage Guide	You must configure the aaa group server tacacs+ command before configuring this command. To configure server address in TACACS+ group server, you must use the tacacs-server host command in global configuration mode. If there is no response from the first host entry, the next host entry is tried.	
Configuration Examples	The following example configures a TACACS+ server group named tac1 and a TACACS+ server address 1.1.1.1 in this group. <pre>FS(config)#aaa group server tacacs+ tac1 FS(config-gs-tacacs+)# server 1.1.1.1</pre>	
Related Commands	Command	Description
	aaa group server tacacs+	Configures a TACACS+ server group.
Platform Description	N/A	

3.6 show tacacs

	Use this command to display the TACACS+ server configuration.	
	show tacacs	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode/Global configuration/Interface configuration mode	
Usage Guide	N/A	

Configuration	The following example displays the TACACS+ server configuration.	
Examples	<pre>FS# show tacacs Tacacs+ Server : 172.19.192.80/49 Socket Opens: 0 Socket Closes: 0 Total Packets Sent: 0 Total Packets Recv: 0 Reference Count: 0</pre>	
Related Commands	Command	Description
	tacacs-server host	Defines a TACACS+ secure server host.
Platform Description	N/A	

3.7 tacacs-server host

	Use this command to configure a TACACS+ host. Use the no form of this command to remove the TACACS+ host.	
	tacacs-server host [oob [<i>via mgmt-name</i>]] { <i>ipv4-address</i> <i>ipv6-address</i> } [port <i>integer</i>] [timeout <i>integer</i>] [key [0 7] <i>text-string</i>]	
	no tacacs-server host { <i>ip-address</i> <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address of the TACACS+ host
	<i>ipv6-address</i>	IPv6 address of the TACACS+ host
	oob [<i>via mgmt-name</i>]	Specifies an MGMT port as the source port for TACACS+ communication.
	port <i>integer</i>	Port number of the server. The range is from 1 to 65,535. The default is 49.
	timeout <i>integer</i>	Timeout time of TACACS+ host. The range is from 1 to 1,000.
	key <i>string</i>	Configures an authentication and encryption key. The value can be 0 or 7. 0 indicates no encryption, while 7 indicates simple encryption. The default is 0.
Defaults	No TACACS+ host is specified by default.	
Command Mode	Global configuration mode	
Usage Guide	The TACACS+ host must be configured to implement AAA security service. You can use this command to configure one or multiple TACACS+ hosts.	

Configuration	The following example configures a TACACS+ host.	
Examples	FS(config)# tacacs-server host 192.168.12.1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

3.8 tacacs-server key

	Use this command to configure the authentication encryption key used for TACACS+ communications between the access server and the TACACS+ server. Use the no form of this command to remove the authentication encryption key.	
	tacacs-server key [0 7] <i>string</i>	
	no tacacs-server key	
Parameter Description	Parameter	Description
	<i>string</i>	Key string
	0 7	Encryption type of key 0 indicates no encryption; 7 indicate simple encryption.
Defaults	No authentication encryption key is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	Use command to configure a global authentication and encryption key for TACACS+ communication. Use the key parameter in the tacacs-server host command to configure a server-based key.	
Configuration	The following example defines the authentication encryption key of TACACS+ server as aaa:	
Examples	FS(config)# tacacs-server key aaa	
Related Commands	Command	Description
	tacacs-server host	Defines a TACACS+ host.
Platform Description	N/A	

3.9 tacacs-server timeout

	Use this command to set the interval for which the server waits for a server host to reply. Use the no form of this command to restore the default timeout interval.	
	tacacs-server timeout <i>seconds</i>	
	no tacacs-server timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Timeout interval in the range from 1 to 1,000 in the unit of seconds
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use command to configure a global timeout interval. Use the timeout parameter in the tacacs-server host command to configure a server-based interval.	
Configuration Examples	The following example configures the timeout interval to 10 seconds. <pre>FS(config)# tacacs-server timeout 10</pre>	
Related Commands	Command	Description
	tacacs-server host	Defines a TACACS+ secure server host.
Platform Description	N/A	

4 802.1X Commands

4.1 aaa authorization ip-auth-mode

	Use this command to set the IP authorization mode.	
	aaa authorization ip-auth-mode { disable supplicant radius-server dhcp-server mixed }	
Parameter	Parameter	Description
Description	disable	Disables IP authorization mode.
	supplicant	Enables supplicant authorization mode.
	radius-server	Enables Radius server authorization mode.
	dhcp-server	Enables DHCP server authorization mode.
	mixed	Enables mixed authorization mode.
Defaults	IP authorization mode is disabled by default.	
Command mode	Global configuration mode	
Usage Guide	Supplicant authorization mode supports only FS supplicant. Radius-server authorization mode requires the server to allocate IP addresses by framed-ip. DHCP-server authorization mode requires the server to enable DHCP snooping or DHCP relay. Mixed authorization mode supports multiple authorization methods.	
Configuration Examples	The following example enables supplicant authentication mode. <pre>FS(config)# aaa authorization ip-auth-mode supplicant</pre>	
Related Commands	Command	Description
	show running-config	Displays the IP authentication mode.
Platform Description	N/A	

4.2 clear dot1x user all

	Use this command to clear all the 802.1X authentication users.	
	clear dot1x user all	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear all the 802.1X authentication users.	
Configuration Examples	The following example clears all the 802.1X authentication users.	
	FS#clear dot1x user all	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.3 clear dot1x user mac

	Use this command to clear 802.1X authentication users according to MAC addresses.	
	clear dot1x user mac <i>mac-addr</i>	
Parameter	Parameter	Description
Description	<i>mac-addr</i>	MAC address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear 802.1X authentication users according to MAC addresses.	
Configuration Examples	The following example clears an 802.1X authentication user whose MAC address is 0012.3456.789A. FS#clear dot1x user mac 0012.3456.789A	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.4 clear dot1x user name

	Use this command to clear the 802.1 X authentication users according to the username.
	clear dot1x user name <i>name-str</i>

Parameter	Parameter	Description
Description	<i>name-str</i>	The username of the 802.1X authentication user
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the 802.1 X authentication users according to the username.	
Configuration Examples	The following example clears the 802.1X authentication user named 802.1X-user. <pre>FS#clear dot1x user name dot1x-user</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.5 clear dot1x user ip

	Use this command to clear 802.1X authentication users according to IP addresses. clear dot1x user ip <i>ip-addr</i>	
Parameter Description	Parameter	Description
	<i>ip-addr</i>	IP address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear 802.1X authentication users according to IP addresses.	
Configuration Examples	The following example clears an 802.1X authentication user whose IP address is 11.1.1.1. <pre>FS#clear dot1x user ip 11.1.1.1</pre>	
Platform Description	N/A	

4.6 dot1x accounting

	Use this command to configure the accounting list.
	dot1x accounting <i>list-name</i>

Parameter	Parameter	Description				
Description	<i>list-name</i>	The name of the accounting list				
Defaults	N/A					
Command Mode	Global configuration mode/WLAN security configuration mode					
Usage Guide	If AAA does not adopts 802.1X accounting as the default accounting method. Use this command to configure the 802.1X accounting method. Configuration in WLAN security configuration mode is prior to that in global configuration mode.					
Configuration Examples	The following example configures the accounting list. FS(config)# dot1x accounting dot1x-acct					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

4.7 dot1x acct-update base-on first-time server

	Use this command to assign the accounting update interval for the first authentication. Use the no form of this command to restore the default settings. dot1x acct-update base-on first-time server no dot1x acct-update base-on first-time server	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The assignment is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Some portal servers do not support the assignment of accounting update interval during re-authentication. Use this command if such servers demand users to issue accounting update packets according to the interval in the first authentication.	
Configuration Examples	The following example assigns the accounting update interval for the first authentication. FS(config)# dot1x acct-update base-on first-time server	
Platform Description	N/A	

4.8 dot1x auth-fail max-attempt

	Use this command to set the maximum auth-attempts. Use the no form of this command to restore the default setting.	
	dot1x auth-fail max-attempt <i>value</i>	
	no dot1x auth-fail max-attempt	
Parameter	Parameter	Description
Description	<i>value</i>	The maximum auth-attempts
Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	Use the show dot1x command to adjust the maximum authentication attempts for those failed users.	
Configuration Examples	The following example sets the maximum auth-attempts to 2. FS(config)# dot1x auth-fail max-attempt 2	
Related Commands	Command	Description
	show dot1x	Displays the 802.1x configuration.
Platform Description	N/A	

4.9 dot1x auth-mode

	Use this command to specify the 802.1X authentication mode.	
	dot1x auth-mode { eap chap pap }	
Parameter	Parameter	Description
Description	eap	Enables EAP-MD5 authentication mode.
	chap	Enables CHAP authentication mode.
	pap	Enables PAP authentication mode.
Defaults	The default is EAP-MD5 authentication mode.	
Command Mode	Global configuration mode	
Usage Guide	The selection of authentication mode depends on the suppliant and portal server.	
Configuration	The following example enables CHAP authentication mode.	

Examples	FS(config)# dot1x auth-mode chap	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform Description	N/A	

4.10 dot1x auth-address-table address

	Use this command to configure the authentication address table.	
	dot1x auth-address-table address <i>mac-addr</i> interface <i>interface</i>	
Parameter Description	Parameter	Description
	<i>mac-addr</i>	The MAC address of the authentication host
	<i>interface</i>	The interface of the authentication host
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Only the specified interface with the specified MAC address is able to pass the 802.1x authentication.	
Configuration Examples	The following example configures the authentication address table. FS(config)# dot1x auth-address-table 00d0.f800.0cb2 interface fastethernet 0/1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.11 dot1x authentication

	Use this command to configure the authentication method list.	
	dot1x authentication <i>list-name</i>	
Parameter Description	Parameter	Description
	<i>list-name</i>	Authentication method list
Defaults	N/A	
Command	Global configuration mode	

Mode		
Usage Guide	If AAA does not adopt the default 802.1X authentication, use this command to configure the 802.1X authentication method.	
Configuration Examples	The following example configures the authentication method list FS(config)# dot1x authentication dot1x-authen	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.12 dot1x auto-req

	Use this command to configure auto-request 802.1X authentication. Use the no form of this command to restore the default setting.	
	dot1x auto-req	
	no dot1x auto-req	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Enable this function for MAB. If the authentication agent is already in the terminal system, enable it by clicking.	
Configuration Examples	The following example enables auto-request 802.1X authentication. FS(config)# dot1x auto-req	
Related Commands	Command	Description
	show dot1x auto-req	Displays the automatic authentication request information.
Platform Description	N/A	

4.13 dot1x auto-req packet-num

	Use this command to set the number of auto-request authentication packets.
	dot1x auto-req packet-num num

Parameter	Parameter	Description
Description	<i>num</i>	The number of auto-request authentication packets in the range from 0 to 1,000,000
Defaults	The default is 0.	
Command Mode	N/A	
Usage Guide	N/A	
Configuration Examples	The following example sets the number of auto-request authentication packets to 100. <pre>FS(config)# dot1x auto-req packet-num 100</pre>	
Related Commands	Command	Description
	show dot1x auto-req	Displays the authentication request information.
Platform Description	N/A	

4.14 dot1x auto-req req-interval

	Use this command to set the auto-request authentication interval.	
	dot1x auto-req req-interval <i>time</i>	
Parameter	Parameter	Description
Description	<i>time</i>	The auto-request authentication interval, in the range from 10 to 3,600 in the unit of seconds
Defaults	The default is 30 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the auto-request authentication interval to 50 seconds. <pre>FS(config)# dot1x auto-req req-interval 50</pre>	
Related Commands	Command	Description
	show dot1x auto-req	Displays the authentication request information.
Platform Description	N/A	

4.15 dot1x auto-req user-detect

	Use this command to enable online user detection for auto-request authentication. Use the no form of this command to disable this function.	
	dot1x auto-req user-detect	
	no dot1x auto-req user-detect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables online user detection for auto-request authentication. FS(config)# dot1x auto-req user-detect	
Related Commands	Command	Description
	show dot1x auto-req	Displays the authentication request information.
Platform Description	N/A	

4.16 dot1x client-probe enable

	Use this command to enable online user probe function. Use the no form of this command to restore the default setting.	
	dot1x client-probe enable	
	no dot1x client-probe enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable online user probe function.	
Configuration	The following example enables online user probe function.	

Examples	FS(config)# dot1x client-probe enable	
Related Commands	Command	Description
	show dot1x	Displays 802.1X configuration.
Platform Description	N/A	

4.17 dot1x critical

	Use this command to enable the server IAB (Inaccessible Authentication Bypass) on the port. Use the no form of this command to restore the default setting.	
	dot1x critical	
	no dot1x critical	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This functions is disabled by default.	
Command Mode	Interface configuration mode/VXLAN mode	
Usage Guide	With the IAB function enabled on the port, if there is only RADIUS authentication method in the 802.1X authentication method list and all RADIUS servers in this method list take no effect, the switch will set the network accessing authority for users by the IAB method, and send the EAPOL-SUCCESS packets to the users. Except for the RADIUS authentication method, if there are other authentication methods in the 802.1X authentication method list, the IAB function will take no effect. (Such as the aaa authentication dot1x default group radius none, there exists none authentication method after the RADIUS authentication method. For the users of IAB authorized, as the user identity legality cannot be checked, no matter whether the accounting function is configured, they will not send the accounting request. With the AAA multi-domain authentication enabled globally, the 802.1X user authentication will not use the globally configured method list. After all RADIUS servers in the 802.1X globally configured method list are checked to be invalid, the IAB will directly send the successful authentication to the user with no need to enter the username, the AAA multi-domain authentication on this port is useless.	
Configuration Examples	The following example enables the server IAB (Inaccessible Authentication Bypass) function on the port. FS(config-if-GigabitEthernet 0/5)#dot1x critical	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.18 dot1x critical recovery action reinitialize

	Use this command to allow IAB users under the port to reinitialize authentication when the server has recovered. Use the no form of this command to restore the default setting.	
	dot1x critical recovery action reinitialize	
	no dot1x critical recovery action reinitialize	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode/VXLAN mode	
Usage Guide	After the port entering the inaccessible authentication bypass status, if the RADIUS server returns to normal, you need to reinitialize the authentication for all users that have accomplished the network access authorization through the inaccessible authentication bypass on ports in order to ensure the user legality.	
Configuration Examples	The following example allows IAB users under the port to reinitialize authentication when the server has recovered. FS(config-if-GigabitEthernet 0/5)#dot1x critical recovery action reinitialize	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.19 dot1x critical vlan

	Use this command to configure the port in IAB status to jump to a specified auth-fail VLAN. Use the no form of this command to disable this function.	
	dot1x critical vlan	
	no dot1x critical vlan	
Parameter	Parameter	Description
Description	<i>vlan-id</i>	The VLAN where the port will jump
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode/VXLAN mode	

Usage Guide	With this function enabled, if no user authentication is performed on the ports initially, after all RADIUS servers are invalidated, the user will initiate the authentication and the port will enter the IAB status and to be added to the VLAN configured. If this function is disabled, the VLAN of the port is not changed when the port is in the IAB status.	
Configuration Examples	The following example configures the port in IAB status to jump to a specified auth-fail VLAN. FS(config-if-GigabitEthernet 0/5)#dot1x critical vlan 10	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.20 dot1x dbg-filter

	Use this command to enable debug information print for a user with a specified MAC address. Use the no form of this command to clear the debug information.	
	dot1x dbg-filter <i>H.H.H</i>	
	no dot1x dbg-filter <i>H.H.H</i>	
Parameter Description	Parameter	Description
	<i>H.H.H</i>	The MAC address of a user
Defaults	Debug information of all authentication users is printed by default.	
Command mode	Global configuration mode	
Usage Guide	Use this command to print the debug information of a specific user If you want to locate the fault on the network where there are multiple users.	
Configuration Examples	The following example prints the debug information of the device with the specified MAC address. FS(config)# dot1x dbg-filter 00d0.f800.0001	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.21 dot1x default-user-limit

	Use this command to set the maximum auth-user number on controlled interfaces.

	Use the no form of this command to restore the default setting.	
	dot1x default-user-limit <i>num</i>	
	no dot1x default-user-limit	
Parameter	Parameter	Description
Description	<i>num</i>	The maximum auth-user number allowed by a controlled interface, in the range from 1 to 1,000,000
Defaults	The default is 1,000,000.	
Command mode	Interface configuration mode/ VXLAN mode	
Usage Guide	This command is used to limit the number of users to be authenticated on a specific port.	
Configuration Examples	The following example sets the maximum auth-user number on a controlled interface.	
	FS(config-if)# dot1x default-user-limit 10	
Related Commands	Command	Description
	show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1X interface.
	show dot1x port-control interface fastEthernet 0/10	Displays the number of users allowed by a specific 802.1X interface.
Platform Description	N/A	

4.22 dot1x default

	Use this command to restore 802.1X configuration to the default setting.	
	dot1x default	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to restore 802.1X configuration for quick re-configuration.	
Configuration Examples	The following example restores 802.1X configuration to the default setting.	
	FS(config)# dot1x default	

Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform Description	N/A	

4.23 dot1x get-static-ip enable

	Use this command to obtain static IP addresses. dot1x get-static-ip enable	
	Use this command to restore the default setting. no dot1x get-static-ip enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Enable this function when wireless terminals use static IP addresses and need to upload the static IP addresses to the server.	
	Note that the IP addresses are uploaded to the server via accounting packets. In addition, when static IP addresses are used, terminal identification information is not provided.	
Configuration Examples	The following example obtains static IP addresses.	
	FS(config)# dot1x get-static-ip enable	
Platform Description	This command is supported only on wireless products.	

4.24 dot1x mab-username upper

	Use this command to enable uppercase letters in MAB user names.	
	dot1x mab-username upper	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Global configuration mode.					
Usage Guide	By default, lowercase letters are used in the user name of MAB. After this function is enabled, uppercase letters are used in new user names of MAB to meet server requirements.					
Configuration Examples	The following example enables uppercase letters in MAB user names. FS(config)# dot1x mab-username upper					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

4.25 dot1x mac-auth-bypass

	Use this command to configure single MAB authentication. Use the no form of this command to restore the default setting.	
	dot1x mac-auth-bypass	
	no dot1x mac-auth-bypass	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command on a single dumb terminal.	
Configuration Examples	The following example configures single MAB authentication. FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass	
Related Commands	Command	Description
	show dot1x port-control interface	Displays the information about 802.1X on the interface.
Platform Description	N/A	

4.26 dot1x mac-auth-bypass multi-user

	Use this command to configure multiple MAB authentications.

	Use the no form of this command to restore the default setting.	
	dot1x mac-auth-bypass multi-user	
	no dot1x mac-auth-bypass multi-user	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode/VXLAN mode	
Usage Guide	Use this command when the interface is connected with multiple dumb terminals.	
Configuration Examples	The following example configures multiple MAB authentications. FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.27 dot1x mac-auth-bypass timeout-activity

	Use this command to set the MAB authentication timeout interval.	
	dot1x mac-auth-bypass timeout-activity <i>time</i>	
	no dot1x mac-auth-bypass timeout-activity	
Parameter	Parameter	Description
Description	<i>time</i>	The online time, in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 0 second.	
Command Mode	Interface configuration mode/VXLAN mode	
Usage Guide	Use this command to set the MAB authentication timeout interval for dumb terminals.	
Configuration Examples	The following example sets the MAB authentication timeout interval. FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass timeout-activity 3600	

Related Commands	Command	Description
	show dot1x port-control interface	Displays the 802.1X information.
	show dot1x port-control interface	Displays the 802.1X information.
Platform Description	N/A	

4.28 dot1x mac-auth-bypass violation

	Use this command to configure the MAB violation. Use the no form of this command to restore the default setting.	
	dot1x mac-auth-bypass violation	
	no dot1x mac-auth-bypass violation	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command is used to configure the MAB violation on the port with only one dumb terminal in single MAB environment.	
Configuration Examples	The following example configures the MAB violation. FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass violation	
Related Commands	Command	Description
	show dot1x port-control interface	Displays the 802.1X information.
Platform Description	N/A	

4.29 dot1x mac-auth-bypass vlan

	Use this command to configure the MAB VLAN function. Use the no form of this command to restore the default setting.	
	dot1x mac-auth-bypass vlan <i>vlan-list</i>	
	no dot1x mac-auth-bypass vlan <i>vlan-list</i>	
Parameter Description	Parameter	Description
	<i>vlan-list</i>	Configures the MAB VLANs.

Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to allow users within specified VLANs on the port to perform MAB authentication.	
Configuration Examples	The following example configures MAB VLANs. FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5, 8-20	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.30 dot1x max-req

	Use this command to set the maximum attempts of authentication requests.	
	dot1x max-req <i>num</i>	
Parameter	Parameter	Description
Description	<i>num</i>	Maximum attempts
Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	Use the show dot1x command to display the 802.1X configuration.	
Configuration Examples	The following example sets the maximum attempts of authentication requests to 2. FS(config)# dot1x max-req 2	
Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.
Platform Description	N/A	

4.31 dot1x multi-account enable

	Use this command to enable the user with one single MAC address to perform authentication with multiple accounts.

	Use the no form of this command to restore the default setting.	
	dot1x multi-account enable	
	no dot1x multi-account enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use the command to enable the multiple-account authentication if you want to switch the username in the authentication or re-authentication, especially in the windows domain authentication.	
Configuration Examples	The following example enables the multiple-account authentication. FS(config)# dot1x multi-account enable	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.32 dot1x multi-mab quiet-period

	Use this command to set the quiet time after the multiple MAB authentication failure.	
	dot1x multi-mab quiet-period <i>time</i>	
Parameter	Parameter	Description
Description	<i>time</i>	Sets the quiet period after the multiple MAB authentication failure, in the range from 0 to 65,535 in the unit of seconds.
Defaults	The default is 0 second, indicating no quiet period.	
Command Mode	Global configuration mode	
Usage Guide	The default setting is recommended.	
Configuration Examples	The following example sets the quiet period after the multiple MAB authentication failure to 2 seconds. FS(config)# dot1x multi-mab quiet-period 2	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.33 dot1x mab-username format

	Use this command to configure the MAB authentication user name format. Use the no form of this command to restore the default setting. dot1x mab-username format [with-dot with-colon with-hyphen] no dot1x mab-username format	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, this function is disabled.	
Command Mode	Global configuration mode	
Usage Guide	dot1x mab-username format with-dot is used to configure the MAB authentication user name format XXXX.XXXX.XXXX. dot1x mab-username format with-colon is used to configure the MAB authentication user name format XX:XX:XX:XX:XX:XX. dot1x mab-username format with-hyphen is used to configure the MAB authentication user name format XX-XX-XX-XX-XX-XX.	
Configuration Examples	The following example configures the MAB authentication user name format. <pre>FS(config)# dot1x mab-username format with-hyphen</pre>	
Platform Description	N/A	

4.34 dot1x port-control auto

	Use this command to configure the 802.1X authentication on the port. Use the no form of this command to restore the default setting. dot1x port-control auto no dot1x port-control	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Interface configuration mode/VXLAN mode	
Usage Guide	Use the show dot1x command to display the 802.1X configuration.	
Configuration Examples	The following example configures the 802.1X authentication on the port. FS(config-if-GigabitEthernet 0/0)# dot1x port-control auto	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform Description	N/A	

4.35 dot1x port-control-mode

	By default, 802.1x adopts MAC address-based control mode. In this mode, only authenticated users have access to the network, while other users that connect to the same port cannot access the network. In the port-based control mode, however, if one user that connects to the port passes the authentication, this port becomes an authenticated port and all the users that connect to this port have access to the network. In the port-based single-user control mode, the port is authenticated when it allows only one authenticated user who is enable to use the network normally. If you find other users on the port, you should clear all the users on the port and re-authenticate. The authentication mode can be configured using the following commands	
	dot1x port-control-mode { mac-based port-based port-based single-host}	
	no dot1x port-control-mode	
Parameter Description	Parameter	Description
	mac-based	Enable the MAC address-based control.
	port-based	Enable port-based control.
	port-based single-host	Enable single host-based control.
Defaults	MAC address-based access control is used by default.	
Command Mode	Interface configuration mode.	
Usage Guide	Use the show dot1x port-control command to show the 802.1X configuration for the port. Single-host is port-based single-user 802.1x access control. Use show dot1x port-control to display port-based and use show running-config to display dot1x port-control-mode port-based single-host. Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.	

Configuration Examples	The following example sets the port to participate in authentication and enable port-based authentication. FS(config-if-GigabitEthernet 0/0)# dot1x port-control-mode port-based	
Related Commands	Command	Description
	show dot1x port-control	Displays the port control mode.
	Show running-config	Displays the configuration.
Platform Description	N/A	

4.36 dot1x probe-timer interval

	Use this command to set the FS terminal detection interval.	
	dot1x probe-timer interval <i>time</i>	
Parameter Description	Parameter	Description
	<i>time</i>	Terminal detection interval in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 20 seconds.	
Command Mode	Global configuration mode	
Usage Guide	The default setting is recommended.	
Configuration Examples	The following example sets FS terminal detection interval to 30 seconds. FS(config)# dot1x probe-timer interval 30	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.37 dot1x probe-timer alive

	Use this command to set the FS terminal alive interval.	
	dot1x probe-timer alive <i>time</i>	
Parameter Description	Parameter	Description
	<i>time</i>	Terminal alive interval, in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 250 seconds.	

Command Mode	Global configuration mode	
Usage Guide	If the device does not receive the probe packet from the terminal when the terminal alive interval expires, the device is considered offline. The default setting is recommended.	
Configuration Examples	The following example sets FS terminal alive interval to 120 seconds. FS(config)# dot1x probe-timer alive 120	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.38 dot1x private-supplicant-only

	Use this command to filter non-FS clients. Use the no form of this command to restore the default setting.	
	dot1x private-suppliant-only	
	no dot1x private-suppliant-only	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used for authentication supporting only FS clients.	
Configuration Examples	The following example filters non-FS clients. FS(config)# dot1x private-suppliant-only	
Related Commands	Command	Description
	show dot1x private-suppliant-only	Displays the information about the private supplicant.
Platform Description	N/A	

4.39 dot1x pseudo source-mac

	Use this command to use a virtual MAC address as the source MAC address of the 802.1X packets sent by the device. Use the no form of this command to restore the default setting.	
	dot1x pseudo source-mac	
	no dot1x pseudo source-mac	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	Global configuration mode	
Usage Guide	By default, the device uses its own MAC address as the source MAC address of the EAP packets for the 802.1X authentication. Some versions of the FS supplicant judge whether the access device is a FS device based on the source MAC address of the EAP packets. If the access device is a FS device, the supplicant device performs some private features. Configure this command if you want to enable these features.	
Configuration Examples	The following example uses the virtual MAC address as the source MAC address of the 802.1X packets sent by the device: <pre>FS(config)# dot1x pseudo source-mac</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.40 dot1x redirect

	Use this command to enable the second generation SU upgrade function. Use the no form of this command to restore the default setting.	
	dot1x redirect	
	no dot1x redirect	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command	Global configuration mode	

Mode		
Usage Guide	Redirect to the supplicant software download website through the browser. See <i>Web Authentication Configuration Guide</i> for details about parameters.	
Configuration Examples	The following example enables the second generation SU upgrade function, FS(config)# dot1x redirect	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.41 dot1x reauth-max

	Use this command to set the maximum re-auth attempts.	
	dot1x reauth-max <i>num</i>	
	no dot1x reauth-max	
Parameter Description	Parameter	Description
	<i>num</i> ,	Maximum re-auth attempts. The range is from 1 to 10.
Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to specify the maximum number of supplicant re-authentications. Use the show dot1x command to display 802.1X configuration.	
Configuration Examples	The following example sets the maximum re-auth attempts to 2. FS(config)# dot1x reauth-max 2	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform Description	N/A	

4.42 dot1x re-authentication

	Use this command to enable timed re-authentication function.
	Use the no form of the command to restore the default setting.

	dot1x re-authentication	
	no dot1x re-authentication	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command will re-authenticate the supplicant periodically after he passes the authentication. Use the show dot1x command to display 802.1X configuration. The default setting is recommended.	
Configuration Examples	The following example enables timed re-authentication function. FS(config)# dot1x re-authentication	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform Description	N/A	

4.43 dot1x stationarity enable

	In the port-based 802.1X control mode, dynamic users can transit freely among the ports by default. Use this command to prevent users from transition. Use the no form of this command to restore the default setting.	
	dot1x stationarity enable	
	no dot1x stationarity enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command must be configured before user authentication. Otherwise, you need re-authenticate all the users.	
Configuration Examples	The following example prevents the user from transiting from 802.1X port to other port. FS(config)# dot1x stationarity enable	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.44 dot1x timeout re-authperiod

	Use this command to set the re-authentication interval when re-authentication is enabled.	
	dot1x timeout re-authperiod <i>time</i>	
Parameter Description	Parameter	Description
	<i>time</i>	Authentication interval, in the range from 1 to 65,535 in the unit of seconds.
Defaults	The default is 3,600 seconds.	
Command Mode	Global configuration mode	
Usage Guide	Use the show dot1x command to display the 802.1X configuration.	
Configuration Examples	The following example sets the re-authentication interval to 2,400 seconds. <pre>FS(config)# dot1x timeout re-authperiod 2400</pre>	
Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.
Platform Description	N/A	

4.45 dot1x timeout quiet-period

	Use this command to set the quiet period when authentication fails.	
	dot1x timeout quiet-period <i>time</i>	
Parameter Description	Parameter	Description
	<i>time</i>	Quiet period, in the range from 1 to 65,535 in the unit of seconds.
Defaults	The default is 10 seconds.	
Command	Global configuration mode	

Mode		
Usage Guide	The default value is recommended.	
Configuration Examples	The following example sets the quiet period after failed authentication. FS(config)# dot1x timeout quiet-period 60	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.46 dot1x timeout supp-timeout

	Use this command to set the authentication timeout between the device and the supplicant.					
	dot1x timeout supp-timeout <i>time</i>					
Parameter Description	<table><tr><th>Parameter</th><th>Description</th></tr><tr><td><i>time</i></td><td>Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.</td></tr></table>	Parameter	Description	<i>time</i>	Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.	
Parameter	Description					
<i>time</i>	Authentication timeout between the device and the supplicant The range is from 1 to 65,535 seconds.					
Defaults	The default is 3 seconds.					
Command Mode	Global configuration mode					
Usage Guide	Use the show dot1x command to show display 802.1X configuration.					
Configuration Examples	The following example sets the authentication timeout between the device and the supplicant to 10s: FS(config)# dot1x timeout supp-timeout 10					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show dot1x</td><td>Displays the information about 802.1x.</td></tr></table>	Command	Description	show dot1x	Displays the information about 802.1x.	
Command	Description					
show dot1x	Displays the information about 802.1x.					
Platform Description	N/A					

4.47 dot1x timeout server-timeout

	Use this command to set the server timeout interval.
	dot1x timeout server-timeout <i>time</i>

Parameter	Parameter	Description
Description	<i>time</i>	The server timeout interval, in the range from 1 to 65,535 in the unit of seconds
Defaults	The default is 5 seconds.	
Command Mode	Global configuration mode	
Usage Guide	By default, the timeout of the 802.1X server is less than that of the Radius server. Use this command to raise the 802.1X timeout so as to exceed the Radius value. For details, see <i>Configuration Guide</i> .	
Configuration Examples	The following example set the server timeout interval to 10 seconds. <pre>FS(config)# dot1x timeout server-timeout 10</pre>	
Related Commands	Command	Description
	show dot1x	Displays the 802.1X information.
Platform	N/A	
Description		

4.48 dot1x timeout tx-period

	Use this command to set the request/id packet re-transmission interval.	
	dot1x timeout tx-period <i>time</i>	
Parameter	Parameter	Description
Description	<i>time</i>	The request/id packet re-transmission interval, in range from 1 to 65,535 in the unit of seconds
Defaults	The default is 3 seconds for switches, and 4 seconds for wireless devices.	
Command Mode	Global configuration mode	
Usage Guide	Use the show dot1x command to display 802.1X configuration.	
Configuration Examples	The following example sets the request/id packet re-transmission interval to 5 seconds. <pre>FS(config)# dot1x timeout tx-period 5</pre>	
Related Commands	Command	Description
	show dot1x	Displays the information about 802.1X.
Platform	N/A	

Description	

4.49 dot1x valid-ip-acct enable

	Use this command to enable IP address-triggered accounting. Use the no form of this command to restore the default setting.	
	dot1x valid-ip-acct enable	
	no dot1x valid-ip-acct enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable accounting only when users obtain valid IP addresses.	
Configuration Examples	The following example enables IP address-triggered accounting. FS(config)#dot1x valid-ip-acct enable	
Platform Description	N/A	

4.50 dot1x valid-ip-acct timeout

	Use this command to configure IP address-triggered accounting timeout. Use the no form of this command to restore the default setting.	
	dot1x valid-ip-acct timeout time	
	no dot1x valid-ip-acct timeout	
Parameter	Parameter	Description
Description		
	<i>time</i>	IP address-triggered accounting timeout in the unit of minutes
Defaults	The default is 5 minutes.	
Command Mode	Global configuration mode	
Usage Guide	The SNMP server will not start accounting until users obtain IP addresses. In this case, use this command to configure the IP address-triggered accounting timeout.	

Configuration	The following example configures IP address-triggered accounting timeout.	
Examples	FS(config)# dot1x valid-ip-acct timeout 10	
Platform		
Description	N/A	

4.51 dot1x system disable

	Use this command to disable global 802.1x. Use the no form of this command to restore the default settings.	
	dot1x system disable	
	no dot1x system disable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	By default, global 802.1x is enabled.	
Command Mode	Global configuration mode	
Usage Guide	(Optional) When the server is unreachable, disable global 802.1x, so users can access the Internet without authentication. After the server resumes reachability, enable global 802.1x, and users have to pass authentication before accessing the Internet.	
Configuration	The following example disables global 802.1x.	
Examples	FS(config)# dot1x system disable	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

4.52 show dot1x

	Use this command to display the 802.1X setting.	
	show dot1x	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode/Global configuration mode/Interface configuration mode	

Mode		
Usage Guide	N/A	
Configuration Examples	The following example displays the 802.1X setting. <pre>FS#show dot1x</pre> 802.1X basic information: <pre> 802.1X Status enable Authentication Mode eap Authorization mode disable Total User Number 0 (exclude dynamic user) Authenticated User Number 0 (exclude dynamic user) Dynamic User Number 0 Re-authentication disable Re-authentication Period 3600 seconds Re-authentication max 3 times Quiet Period 10 seconds Tx Period 30 seconds Supplicant Timeout 3 seconds Server Timeout 5 seconds Maximum Request 3 times Client Online Probe disable Eapol Tag enable 802.1x redirect disable Private supplicant only disable </pre>	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.
Platform Description	N/A	

4.53 show dot1x auth-address-table

	Use this command to display 802.1X authentication address table.	
	show dot1x auth-address-table [address <i>addr</i> interface <i>interface</i>]	
Parameter	Parameter	Description
Description	<i>addr</i>	Physical IP address that can be authenticated
	<i>interface</i>	Interface number
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the 802.1X authentication address table. <pre> FS #show dot1x auth-address-table Interface Address ----- Fa0/1 00d0.f800.0c0e Fa0/2 001a.c800.0102 FS #show dot1x auth-address-table interface fastEthernet 0/1 Interface Address ----- Fa0/1 00d0.f800.0c0e FS #show dot1x auth-address-table address 00d0.f8.00.0c0e Interface Address ----- Fa0/1 00d0.f800.0c0e </pre>	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1x authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.

	dot1x timeout tx-period	Sets the re-transmission interval.
Platform	N/A	
Description		

4.54 show dot1x auto-req

	Use this command to display the auto-request authentication information.	
	show dot1x auto-req	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the auto-request authentication information. <pre>FS# show dot1x auto-req Auto-Req: Enabled User-Detect : Enabled Packet-Num : 0 Req-Interval: 30 Seconds</pre>	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.
Platform	N/A	
Description		

4.55 show dot1x max-req

	Use this command to display the maximum number of request/challenge packet transmission.	
	show dot1x max-req	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the maximum number of request/challenge packet transmission. <pre>FS#show dot1x max-req</pre> Max-Req: 3 Times	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.
Platform Description	N/A	

4.56 show dot1x port-control

	Use this command to display the port-control information.
	show dot1x port-control [interface interface-type interface-number]

Parameter	Parameter	Description
Description	<i>interface-type</i>	Interface type
	<i>interface-number</i>	Interface ID
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the port-control information. <pre>FS#show dot1x port-control Interface Mode Dynamic-User Static-User Max-User Authened MAB ----- Gi0/5 mac-based 0 0 unlimited no disable</pre>	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.
Platform Description	N/A	

4.57 show dot1x private-suppliant-only

	Use this command to display the information about the private supplicant.	
	show dot1x private-suppliant-only	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information about the private supplicant: <pre>FS#show dot1x private-suppliant-only</pre> <pre>private-suppliant-only: Disabled</pre>	
Related Commands	Command	Description
	dot1x auth-mode	Sets the 802.1X authentication mode.
	dot1x max-req	Sets the maximum number of authentication request re-transmissions.
	dot1x port-control auto	Sets the port to participate in authentication.
	dot1x reauth-max	Sets the maximum number of the supplicant re-authentications.
	dot1x re-authentication	Sets the re-authentication attribute.
	dot1x timeout quiet-period	Sets the time the device waits before re-authentication.
	dot1x timeout re-authperiod	Sets the re-authentication period for the supplicant.
	dot1x timeout server-timeout	Sets the authentication timeout between the device and authentication server.
	dot1x timeout supp-timeout	Sets the authentication timeout between the device and the supplicant.
	dot1x timeout tx-period	Sets the re-transmission interval.
Platform Description	N/A	

4.58 show dot1x probe-timer

	Use this command to display the configuration of online user probe.	
	show dot1x probe-timer	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	

Configuration	The following example displays the configuration of online user probe.	
Examples	FS#show dot1x probe-timer Hello Interval : 20 Hello Alive : 60	
	Field Description	
	Command	Description
	Hello Interval	Sets the probe period.
	Hello Alive	Sets the probe alive interval.
Related	Command	Description
Commands	N/A	N/A.
Platform	N/A	
Description		

4.59 show dot1x re-authentication

	Use this command to display re-authentication status.					
	show dot1x re-authentication					
Parameter	Parameter	Description				
Description	N/A	N/A				
Defaults	N/A					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode					
Usage Guide	N/A					
Configuration Examples	The following example displays re-authentication status. FS#show dot1x re-authentication Reauth-Enabled: Disabled <table><tr><th>Command</th><th>Description</th></tr><tr><td>Reauth-Enabled</td><td>Whether to enable re-authentication.</td></tr></table>		Command	Description	Reauth-Enabled	Whether to enable re-authentication.
Command	Description					
Reauth-Enabled	Whether to enable re-authentication.					
Related Commands	Command	Description				
	N/A	N/A				
Platform Description	N/A					

4.60 show dot1x reauth-max

	Use this command to display the maximum re-auth attempts.	
	show dot1x reauth-max	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the maximum re-authentication attempts. <pre>FS#show dot1x reauth-max</pre> Reauth-Max: 3 Times	
	Command	Description
	Reauth-Enabled	Sets the maximum re-authentication attempts.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.61 show dot1x summary

	Use this command to display the 802.1X authentication summary.	
	show dot1x summary	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	It is convenient to display the 802.1X authentication summary according to the MAC address or username.	
Configuration Examples	The following example displays the summary of 802.1X authentication. <pre>FS#show dot1x summary</pre>	

	ID	User	MAC	Interface	VLAN	INNER-VLAN	Auth-State	Backend-State
	Port-Status	User-Type	Time					
Related Commands	Command			Description				
	dot1x auth-mode			Sets the 802.1X authentication mode.				
	dot1x max-req			Sets the maximum number of authentication request re-transmissions.				
	dot1x port-control auto			Sets the port to participate in authentication.				
	dot1x reauth-max			Sets the maximum number of the supplicant re-authentications.				
	dot1x re-authentication			Sets the re-authentication attribute.				
	dot1x timeout quiet-period			Sets the time the device waits before re-authentication.				
	dot1x timeout re-authperiod			Sets the re-authentication period for the supplicant.				
	dot1x timeout server-timeout			Sets the authentication timeout between the device and authentication server.				
	dot1x timeout supp-timeout			Sets the authentication timeout between the device and the supplicant.				
	dot1x timeout tx-period			Sets the re-transmission interval.				
Platform Description	N/A							

4.62 show dot1x timeout quiet-period

	Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.	
	show dot1x timeout quiet-period	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the time for the device to wait before re-authentication quiet period after the authentication failure.	
Configuration Examples	The following example shows how to displays the quiet period the time for the device to wait before re-authentication after the authentication failure.	
	FS#show dot1x timeout quiet-period	

	Quiet-Period: 10 Seconds	
	Parameter Description:	
	Parameter	Description
	Quiet-Period	The time for the device to wait before re-authentication after the authentication failure.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.63 show dot1x timeout re-authperiod

	Use this command to display the re-authentication interval.					
	show dot1x timeout re-authperiod					
Parameter	Parameter	Description				
Description	N/A	N/A				
Defaults	N/A					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode					
Usage Guide	Use this command to display the re-authentication interval.					
Configuration Examples	The following example displays the re-authentication interval.: <pre>FS#show dot1x timeout re-authperiod</pre> Reauth-Period: 3600 Seconds Parameter Description: <table><tr><th>Parameter</th><th>Description</th></tr><tr><td>Reauth-Period</td><td>Re-authentication interval.</td></tr></table>		Parameter	Description	Reauth-Period	Re-authentication interval.
Parameter	Description					
Reauth-Period	Re-authentication interval.					
Related Commands	Command	Description				
	N/A	N/A				
Platform Description	N/A					

4.64 show dot1x timeout server-timeout

	Use this command to display the authentication timeout period.

	show dot1x timeout server-timeout					
Parameter	Parameter	Description				
Description	N/A	N/A				
Defaults	N/A					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode					
Usage Guide	Use this command to display the authentication timeout period.					
Configuration Examples	Use this command to display the authentication timeout period: FS#show dot1x timeout server-timeout Server-Timeout: 5 Seconds Parameter Description: <table><tr><td>Parameter</td><td>Description</td></tr><tr><td>Server-Period</td><td>AuthenticationServer timeout periodinterval.</td></tr></table>		Parameter	Description	Server-Period	AuthenticationServer timeout periodinterval.
Parameter	Description					
Server-Period	AuthenticationServer timeout periodinterval.					
Related Commands	Command	Description				
	N/A	N/A				
Platform Description	N/A					

4.65 show dot1x timeout supp-timeout

	Use this command to display the request/challenge packets re-transmission interval.	
	show dot1x timeout supp-timeout	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use this command to display the request/challenge packets re-transmission interval.	
Configuration Examples	Use this command to display the request/challenge packets re-transmission interval: <pre>FS#show dot1x timeout supp-timeout</pre>	

	Supp-Timeout: 3 Seconds	
	Field Description:	
	Field	Description
	Server-Period	The request/challenge packets re-transmission interval.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.66 show dot1x timeout tx-period

	Use this command to display the request/id packets re-transmission interval.					
	show dot1x timeout tx-period					
Parameter	Parameter	Description				
Description	N/A	N/A				
Defaults	N/A					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode					
Usage Guide	Use this command to display the request/id packets re-transmission interval.					
Configuration Examples	Use this command to display the request/ id packets re-transmission interval: FS#show dot1x timeout tx-period Tx-Period: 30 Seconds Parameter Description: <table><tr><th>Parameter</th><th>Description</th></tr><tr><td>Tx-Period</td><td>Request/id packets re-transmission interval.</td></tr></table>		Parameter	Description	Tx-Period	Request/id packets re-transmission interval.
Parameter	Description					
Tx-Period	Request/id packets re-transmission interval.					
Related Commands	Command	Description				
	N/A	N/A				
Platform Description	N/A					

4.67 show dot1x user mac

	Use this command to display the information about 802.1X authentication users based on MAC addresses.

	show dot1x user mac mac-addr																					
Parameter	Parameter	Description																				
Description	mac-addr	MAC address																				
Defaults	N/A																					
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode																					
Usage Guide	Use the show dot1x summary command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its MAC address.																					
Configuration Examples	The following example displays the information about the 802.1X authentication user according to the user's MAC address. <pre>FS#show dot1x user mac 0023.aeea.4286</pre> User name: ts-user User id: 16777225 Type: static Mac address is 0023.aeea.4286 Vlan id is 2 Access from port Gi0/5 Time online: 0days 0h 0m17s User ip address is 192.168.3.21 Max user number on this port is 0 Authorization session time is 1000 seconds Supplicant is private Start accounting Permit proxy user Permit dial user IP privilege is 0 user acl-name ts-user_6_0_0 : Parameter Description: <table><tr><th>Parameter</th><th>Description</th></tr><tr><td>User name</td><td>User name</td></tr><tr><td>User id</td><td>User ID</td></tr><tr><td>Type</td><td>User type</td></tr><tr><td>Mac address</td><td>User's MAC address</td></tr><tr><td>Vlan id</td><td>User VLAN ID</td></tr><tr><td>Access from port</td><td>The port that user access from</td></tr><tr><td>Time online</td><td>User online time</td></tr><tr><td>User ip address</td><td>User IP address</td></tr><tr><td>Max user number on this port</td><td>The maximum number of users on the port</td></tr></table>		Parameter	Description	User name	User name	User id	User ID	Type	User type	Mac address	User's MAC address	Vlan id	User VLAN ID	Access from port	The port that user access from	Time online	User online time	User ip address	User IP address	Max user number on this port	The maximum number of users on the port
Parameter	Description																					
User name	User name																					
User id	User ID																					
Type	User type																					
Mac address	User's MAC address																					
Vlan id	User VLAN ID																					
Access from port	The port that user access from																					
Time online	User online time																					
User ip address	User IP address																					
Max user number on this port	The maximum number of users on the port																					

	Authorization session time	The authorized session time
	Supplicant is private	Whether the terminal is a FS device
	Start accounting	The accounting is enabled.
	Permit proxy user	The user is allowed to use the proxy.
	Permit dial user	The user is allowed to dial.
	IP privilege	The IP privilege level
	user acl-name	The ACL information
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

4.68 show dot1x user name

	Use this command to display information about 802.1X authentication users based on usernames.	
	show dot1x user name <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	User name
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode	
Usage Guide	Use the show dot1x summary command to display 802.1X authentication summaries. And use this command to display detailed information of a specific user based on its username.	
Configuration Examples	The following example displays the information about the 802.1X authentication user according to the user name. <pre>FS#show dot1x user name ts-user User name: ts-user User id: 16777225 Type: static Mac address is 0023.aeaa.4286 Vlan id is 2 Access from port Gi0/5 Time online: 0days 0h 0m17s User ip address is 192.168.3.21 Max user number on this port is 0 Authorization session time is 1000 seconds</pre>	

	Supplicant is private	
	Start accounting	
	Permit proxy user	
	Permit dial user	
	IP privilege is 0	
	user acl-name ts-user_6_0_0 :	
	Parameter Description:	
	Parameter	Description
	User name	User name
	User id	User ID
	Type	User type
	Mac address	User's MAC address
	Vlan id	User VLAN ID
	Access from port	The port that user access from
	Time online	User online time
	User ip address	User IP address
	Max user number on this port	The maximum number of users on the port
	Authorization session time	The authorized session time
	Supplicant is private	Whether the terminal is a FS device.
	Start accounting	The accounting is enabled.
Permit proxy user	The user is allowed to use the proxy.	
Permit dial user	The user is allowed to dial.	
IP privilege	The IP privilege level.	
user acl-name	The ACL information.	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5 Web Authentication Commands

5.1 accounting

	Use this command to set an accounting method for the template. Use the no form of this command to restore the default setting.	
	accounting { <i>method-list</i> }	
	no accounting	
Parameter Description	Parameter	Description
	<i>method-list</i>	Name of the method list
Defaults	N/A	
Command Mode	Template configuration mode	
Usage Guide	The <i>method-list</i> parameter in this command should be consistent with network accounting list name configured in AAA.	
Configuration Examples	The following example sets the mlist1 accounting method for the eportalv2 template. FS(config.tmplt.eportalv2)# accounting mlist1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.2 authentication

	Use this command to set an authentication method for the template. Use the no form of this command to restore the default setting.	
	authentication { <i>method-list</i> }	
	no authentication	
Parameter Description	Parameter	Description
	<i>method-list</i>	Name of the method list
Defaults	N/A	

Command Mode	Template configuration mode	
Usage Guide	The <i>method-list</i> parameter in this command should be consistent with the Web authentication method list configured in AAA. The first generation authentication does not support the authentication method list configuration.	
Configuration Examples	The following example sets the mlist1 authentication method for the eportalv2 template. <pre>FS(config.tmplt.eportalv2)#authentication mlist1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.3 bindmode

	Use this command to set a binding mode for the template. Use the no form of this command to restore the default setting.	
	bindmode { ip-mac-mode ip-only-mode }	
	no bindmode	
Parameter Description	Parameter	Description
	ip-mac-mode	IP+MAC mode. The device will write both the IP address information and the MAC address information into the forwarding entry.
	ip-only-mode	IP only mode. The device writes only the IP address information into the forwarding entry. On the L3 network, it is recommended to adopt this mode in case that the MAC address is inaccurate.
Defaults	The default is ip-mac-mode .	
Command Mode	Template configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example adopts the IP only mode for the eportalv2 template. <pre>FS(config.tmplt.eportalv2)# bindmode ip-only-mode</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.4 clear web-auth direct-arp

	Use this command to clear all ARP resources exempt from authentication.	
	clear web-auth direct-arp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears all ARP resources exempt from authentication. <pre>FS# clear web-auth direct-arp</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.5 clear web-auth direct host

	Use this command to clear all authentication-exempted users.	
	clear web-auth direct-host [range]	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	

Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears all authentication-exempted users. FS# clear web-auth direct-host	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.6 clear web-auth direct-site

	Use this command to clear all authentication-exempted network resources.	
	clear web-auth direct-site [range]	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears all authentication-exempted network resources. FS# clear web-auth direct-site	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.7 clear web-auth user

	Use this command to force the user to go offline.

	clear web-auth user { all ip { ip-address ipv6-address } mac mac-address name name-string }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Specifies the user's IPv4 address.
	<i>ipv6-address</i>	Specifies the user's IPv6 address.
	<i>mac-address</i>	Specifies the user's MAC address.
	<i>name-string</i>	Specifies the user name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example forces all users to go offline. FS(config) clear web-auth user all	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.8 fmt

	Use this command to set the URL redirection format in the second template configuration mode. fmt { cmcc-ext1 cmcc-ext2 cmcc-normal }	
	Use this command to set the URL redirection format in the first template configuration mode. fmt { ace FS custom }	
Parameter Description	Parameter	Description
	cmcc-ext1	Extended CMCC format
	cmcc-ext2	Liaoning CMCC format
	cmcc-normal	Standard CMCC format
Defaults	The default URL redirection format is FS format.	
Command Mode	Template configuration mode	

Usage Guide	Use this command to set the URL redirection format based on the corresponding portal standard.
Configuration Examples	The following example sets the URL redirection format to extended CMCC format. FS(config.tmplt.eportalv2)#fmt cmcc-ext1
Platform Description	N/A

5.9 http redirect direct-arp

	Use this command to set the address range of the authentication-exempted ARP. Use the no form of this command to restore the default setting.	
	http redirect direct-arp { <i>ip-address</i> [<i>ip-mask</i>] }	
	no http redirect direct-arp { <i>ip-address</i> [<i>ip-mask</i>] }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address
	<i>ip-mask</i>	(Optional) IPv4 mask
Defaults	No authentication-exempted ARP resource is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	The user cannot learn the ARPs of devices such as the gateway with the ARP CHECK function enabled. Use this command to enable the device to learn the ARP within a specified IP address range without authentication.	
Configuration Examples	The following example sets the IP address 172.16.0.1 as the authentication-exempted ARP resource. FS(config)# http redirect direct-arp 172.16.0.1	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.10 http redirect direct-site

	Use this command to set the range of authentication-exempted network resources. Use the no form of this command to restore the default setting.
	http redirect direct-site { <i>ipv6-address</i> <i>ipv4-address</i> [<i>ip-mask</i>] [arp] <i>mac-address</i> <i>range startip-address</i>

	<i>endip-address</i> } [description <i>description-str</i>] [group <i>group-name</i>]	
	no http redirect direct-site { <i>ipv6-address</i> <i>ipv4-address</i> [<i>ip-mask</i>] <i>mac-address</i> range <i>startip-address</i> <i>endip-address</i> }	
Parameter Description	Parameter	Description
	<i>ipv6-address</i>	IPv6 address of the authentication-exempted network resources
	<i>ip-address</i>	IPv4 address of the authentication-exempted network resources
	<i>ip-mask</i>	IPv4 address mask of the authentication-exempted network resources (optional)
	arp	If the ARP Check is enabled on the access device, the keyword arp is needed for ARP binding of the authentication-exempted network resources (optional). It is necessary for IPv4 network resources only.
	<i>mac-address</i>	MAC address of the authentication-exempted user
	<i>startip-address</i>	Start IP address of the authentication-exempted user
	<i>endip-address</i>	End IP address of the authentication-exempted user
	<i>group-name</i>	Group name of the authentication-exempted user
	<i>description-str</i>	Description of the authentication-exempted user
Defaults	No authentication-exempted network resource is set.	
Command Mode	Global configuration mode	
Usage Guide	When Web/802.1x authentication is enabled, all users must pass Web/client authentication to access network resources. This command is used to make certain network resources available to unauthenticated users. All users can access the authentication-exempted Web sites. Up to 50 authentication-exempted users are supported.	
Configuration Examples	The following example sets the Web site with IP address 172.16.0.1 as the authentication-exempted resource. <pre>FS(config)# http redirect direct-site 172.16.0.1</pre> The following example sets the Web site with MAC address 0000:5e00:0101 as the authentication-exempted resource. <pre>FS(config)# http redirect direct-site 0000:5e00:0101</pre> The following example sets the range from 10.0.0.1 to 12.0.0.1 as authentication-exempted network resources. <pre>FS(config)# http redirect direct-site range 10.0.0.1 12.0.0.1</pre>	
Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.
Platform Description	N/A	

5.11 http redirect port

	Use this command to redirect users' HTTP redirection request to a certain destination port. Use the no form of this command to restore the default setting.	
	http redirect port <i>port-num</i>	
	no http redirect port <i>port-num</i>	
Parameter Description	Parameter	Description
	<i>port-num</i>	Destination port of the HTTP request
Defaults	The default is port 80.	
Command Mode	Global configuration mode	
Usage Guide	When you access the network resource, you send HTTP packets. The access device can intercept such HTTP packets to detect your access. If the access device detects that an unauthenticated user is accessing the network resource, it stops the users with an authentication page/client download page. By default, the access device intercepts users' HTTP packets with port 80 to check whether they are accessing network resources. This command is used to change the destination port of HTTP packets that are intercepted by the access device. Up to 10 ports can be configured, excluding port 80 and port 443.	
Configuration Examples	The following example redirects users' HTTP requests with port 8080. <pre>FS(config)# http redirect port 8080</pre> The following example does not redirect users' HTTP requests with port 80. <pre>FS(config)# no http redirect port 80</pre>	
Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.
Platform Description	N/A	

5.12 http redirect session-limit

	Use this command to set the total number of HTTP sessions that can be originated by an unauthenticated user, or the maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port. Use the no form of this command to restore the default setting.	
	http redirect session-limit <i>session-num</i> [port <i>port-session-num</i>]	
	no http redirect session-limit	

Parameter Description	Parameter	Description
	<i>session-num</i>	Total number of HTTP sessions that can be originated by an unauthenticated user, in the range from 1 to 255.
	<i>port-session-num</i>	The maximum number of HTTP sessions that can be originated by an unauthenticated user connected to each port, in the range from 1 to 65535.
Defaults	Totally 255 HTTP sessions can be originated by an unauthenticated user, and 300 HTTP sessions that can be originated by an unauthenticated user connected to each port.	
Command Mode	Global configuration mode	
Usage Guide	To prevent HTTP attacks caused by unauthenticated users from using up the TCP connections of the access device, the maximum number of HTTP sessions by unauthenticated users must be limited on the access device. In addition to authentication, other programs may also occupy HTTP sessions. Therefore, it is not recommended that the maximum number of HTTP sessions by unauthenticated users be 1	
Configuration Examples	The following example sets the maximum number of HTTP sessions originated by an unauthenticated user to 4. <pre>FS(config)# http redirect session-limit 4</pre>	
Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.
Platform Description	N/A	

5.13 http redirect timeout

	Use this command to set the timeout for the redirection connection maintenance. Use the no form of this command to restore the default setting.	
	http redirect timeout <i>seconds</i>	
	no http redirect timeout	
Parameter Description	Parameter	Description
	<i>seconds</i>	Set the timeout for the redirection connection maintenance, in the range from 1 to 10 in the unit of seconds.
Defaults	The default is 3 seconds.	
Command	Global configuration mode	

Mode		
Usage Guide	This command is used to set the timeout for the redirection connection maintenance. After the three-way handshake succeeds, the redirection connection is maintained until the user sends an HTTP GET/HEAD packet and the system returns an HTTP redirection packet. This timeout is set to prevent users from occupying TCP connections for long without sending any GET/HEAD packets.	
Configuration Examples	The following example sets the timeout for the redirection connection maintenance to 4 seconds. FS(config)# http redirect timeout 4	
Related Commands	Command	Description
	show http redirect	Displays the HTTP redirection configuration.
Platform Description	N/A	

5.14 ip

	Use this command to set an IP address for the portal server. Use the no form of this command to restore the default setting.	
	port { <i>ip-address</i> }	
	no port	
Parameter Description	Parameter	Description
	<i>ip-address</i>	The IPv4 address of the portal server
Defaults	No IP address is set for the portal server by default.	
Command Mode	Template configuration mode	
Usage Guide	This command takes place of the http redirect [<i>ip-address</i>] command, which is now hidden as a compatible command.	
Configuration Examples	The following example sets the IP address of the eportalv1 template to 172.16.0.1. FS(config.tmplt.eportalv1)#ip 172.16.0.1 FS(config.tmplt.eportalv1)#	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

5.15 ip portal source-interface

	Use this command to specify a communication port for the portal server. Use the no form of this command to restore the default setting.	
	ip portal source-interface <i>interface-type interface-num</i>	
	no ip portal source-interface	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Port type
	<i>interface-num</i>	Port No.
Defaults	No communication interface is specified by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example specifies an aggregate port as the communication port. FS (config)# ip portal source-interface Aggregateport 1	
Platform Description	N/A	

5.16 port

	Use this command to set a surveillance port for the portal server. Use the no form of this command to restore the default setting.	
	port { <i>port-num</i> }	
	no port	
Parameter Description	Parameter	Description
	<i>port</i>	The surveillance port of the portal server, which is on only the 2nd generation portal server,
Defaults	The default is 50100 based on the UDP protocol.	
Command Mode	Template configuration mode	

Usage Guide	N/A				
Configuration Examples	The following example sets the surveillance port number of the eportalv2 server to 10000. FS(config.tmplt.eportalv2)#port 10000				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A
Command	Description				
N/A	N/A				
Platform Description	N/A				

5.17 redirect

	Use this command to specify the encapsulation format of the Web-auth URL. redirect { http js } no redirect	
Parameter Description	Parameter	Description
	http	HTTP encapsulation format
	js	Java Script encapsulation format
Defaults	The default encapsulation format is Java Script.	
Command Mode	Template configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example specifies HTTP as the encapsulation format of the Web-auth URL. FS(config.tmplt.eportalv2)#redirect http	
Platform Description	N/A	

5.18 show web-auth acl

	Use this command to display whitelist configuration. show web-auth acl [white-url]

Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode	
Usage Guide	The command is used to check the whitelist configuration of web authentication.	
Configuration Examples	The following example displays whitelist configuration. <pre>FS# show web-auth acl</pre> White URL List:0 -----	
Platform Description	N/A	

5.19 show web-auth authmng

	Use this command to display authentication experience data. show web-auth authmng [statistic abnormal]	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays authentication experience data. FS# show web-auth authmng statistic	
	The following example displays abnormal authentication experience data. FS# show web-auth authmng abnormal record num:0, value:3000, max-num:1000, clock:1	
	Field	Description
	record num	Number of records.

	value	Timeout period in the unit of ms. By default, one abnormal record is generated when the timeout exceeds 3s.
	max-num	Maximum number of records.
	clock	The time when the record is written into flash in the range from 0 o'clock to 23 o'clock. The default time is 1 o'clock.
	Abnormal records are stored in the directory: /data/security/authmanage/webauth/.	
Platform Description	N/A	

5.20 show web-auth control

	Use this command to display the authentication configuration.			
	show web-auth control			
Parameter Description	Parameter	Description		
	N/A	N/A		
Defaults	N/A			
Command Mode	Privileged EXEC mode			
Usage Guide	N/A			
Configuration Examples	The following example displays the authentication configuration and statistics information on the interface.			
	FS(config)#show web-auth control			
	Port	Control	Server Name	Online User Count

	GigabitEthernet 0/1	On	<not configured>	0
	FS(config)#			
	Field		Description	
	Port		Name of the authentication port.	
	Control		Displays whether the Web authentication is enabled on the port or not.	
Server Name		The customized server name on the port. <not configured> indicates the server name has not been configured.		
Online User Count		The number of online users on this port.		
Related Commands	Command		Description	
	N/A		N/A	

Platform	N/A
Description	

5.21 show web-auth direct-arp

	Use this command to display the address range of the authentication-exempted ARP.															
	show web-auth direct-arp															
Parameter Description	Parameter	Description														
	N/A	N/A														
Defaults	N/A															
Command Mode	Privileged EXEC mode															
Usage Guide	I N/A															
Configuration Examples	The following example displays the address range of the authentication-exempted ARP. FS(config)#show web-auth direct-arp Direct arps: <table><tr><td>Address</td><td>Mask</td></tr><tr><td>-----</td><td></td></tr><tr><td>1.1.1.1</td><td>255.255.255.255</td></tr><tr><td>2.2.2.2</td><td>255.255.255.255</td></tr></table> FS(config)# <table><tr><th>Field</th><th>Description</th></tr><tr><td>Address</td><td>IPv4 address.</td></tr><tr><td>Mask</td><td>IPv4 mask.</td></tr></table>		Address	Mask	-----		1.1.1.1	255.255.255.255	2.2.2.2	255.255.255.255	Field	Description	Address	IPv4 address.	Mask	IPv4 mask.
Address	Mask															

1.1.1.1	255.255.255.255															
2.2.2.2	255.255.255.255															
Field	Description															
Address	IPv4 address.															
Mask	IPv4 mask.															
Related Commands	Command	Description														
	N/A	N/A														
Platform Description	N/A															

5.22 show web-auth direct-host

	This command is used to display the Web authentication-exempted users.
	show web-auth direct-host

Parameter Description	Parameter		Description																																	
	N/A		N/A																																	
Defaults	N/A																																			
Command Mode	Privileged EXEC mode																																			
Usage Guide	N/A																																			
Configuration Examples	The following example displays the Web authentication-exempted users.																																			
	FS# show web-auth direct-host																																			
	Direct hosts:																																			
	<table><tr><td>Address</td><td>Mask</td><td>Port</td><td>ARP Binding</td><td>Group</td><td>Description</td></tr><tr><td colspan="6">-----</td></tr><tr><td>192.168.0.1</td><td>255.255.255.255</td><td>Gi0/2</td><td>On</td><td>N/A</td><td>N/A</td></tr><tr><td>192.168.4.11</td><td>255.255.255.255</td><td>Gi0/10</td><td>On</td><td>N/A</td><td>N/A</td></tr><tr><td>192.168.5.0</td><td>255.255.255.0</td><td>Gi0/16</td><td>Off</td><td>N/A</td><td>N/A</td></tr></table>						Address	Mask	Port	ARP Binding	Group	Description	-----						192.168.0.1	255.255.255.255	Gi0/2	On	N/A	N/A	192.168.4.11	255.255.255.255	Gi0/10	On	N/A	N/A	192.168.5.0	255.255.255.0	Gi0/16	Off	N/A	N/A
	Address	Mask	Port	ARP Binding	Group	Description																														

	192.168.0.1	255.255.255.255	Gi0/2	On	N/A	N/A																														
	192.168.4.11	255.255.255.255	Gi0/10	On	N/A	N/A																														
	192.168.5.0	255.255.255.0	Gi0/16	Off	N/A	N/A																														
Field		Description																																		
Address		IP address of the user free of authentication																																		
Mask		IP address mask of the user free of authentication																																		
Port		Access device port that is bound with the user's IP address																																		
ARP Binding		Enable/Disable ARP binding																																		
Related Commands	Command			Description																																
	N/A			N/A																																
Platform Description	N/A																																			

5.23 show web-auth direct site

	Use this command to display the range of the Web authentication-exempted network resources.	
	show web-auth direct-site	
Parameter Description	Parameter	Description

	N/A	N/A																	
Defaults	No network resource without authentication is set.																		
Command Mode	Privileged EXEC mode																		
Usage Guide	N/A																		
Configuration Examples	The following example displays the range of the Web authentication-exempted network resources without authentication. FS(config)#show web-auth direct-site Direct sites: <table><thead><tr><th>Address</th><th>Mask</th><th>ARP Binding</th></tr></thead><tbody><tr><td>1.1.1.1</td><td>255.255.255.255</td><td>Off</td></tr><tr><td>2.2.2.2</td><td>255.255.255.255</td><td>On</td></tr></tbody></table> FS(config)# <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Address</td><td>IP address.</td></tr><tr><td>Mask</td><td>IP mask.</td></tr><tr><td>ARP Binding</td><td>Displays whether the ARP binding function is enabled.</td></tr></tbody></table>		Address	Mask	ARP Binding	1.1.1.1	255.255.255.255	Off	2.2.2.2	255.255.255.255	On	Field	Description	Address	IP address.	Mask	IP mask.	ARP Binding	Displays whether the ARP binding function is enabled.
Address	Mask	ARP Binding																	
1.1.1.1	255.255.255.255	Off																	
2.2.2.2	255.255.255.255	On																	
Field	Description																		
Address	IP address.																		
Mask	IP mask.																		
ARP Binding	Displays whether the ARP binding function is enabled.																		
Related Commands	Command	Description																	
	N/A	N/A																	
Platform Description	N/A																		

5.24 show web-auth parameter

	Use this command to display the HTTP redirect configuration.	
	show web-auth parameter	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A						
Configuration Examples	The following example displays the HTTP redirect configuration <pre>FS# show web-auth parameter session-limit: 10 timeout: 5</pre> <table> <tr> <th>Field</th><th>Description</th></tr> <tr> <td>session-limit</td><td>Total number of HTTP sessions that are created by an unauthenticated user.</td></tr> <tr> <td>timeout</td><td>Timeout interval of the redirection connection.</td></tr> </table>	Field	Description	session-limit	Total number of HTTP sessions that are created by an unauthenticated user.	timeout	Timeout interval of the redirection connection.
Field	Description						
session-limit	Total number of HTTP sessions that are created by an unauthenticated user.						
timeout	Timeout interval of the redirection connection.						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>N/A</td><td>N/A</td></tr> </table>	Command	Description	N/A	N/A		
Command	Description						
N/A	N/A						
Platform Description	N/A						

5.25 show web-auth portal-check

	Use this command to display the portal-check configuration. show web-auth portal-check	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the portal-check configuration. <pre>FS#sh web portal-check Check: Enable Interval: 3s Timeout: 5s Retransmit: 3 Escape: Enable Nokick: Disable</pre>	

Platform Description	N/A

5.26 show web-auth rdport

	Use this command to display the TCP interception port.	
	show web-auth rdport	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the TCP interception port. <pre>FS#show web-auth rdport Rd-Port: 80 443 FS#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.27 show web-auth syslog ip

	Use this command to display online and offline records about users.	
	show web-auth syslog ip <i>ip-address</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	A user's IP address.
Defaults	N/A	

Command Mode	Privileged EXEC mode																					
Usage Guide	This command cannot be used to save original data after hot backup.																					
Configuration Examples	The following example displays online and offline records of users. <pre>FS#show web-auth syslog ip 192.168.197.35 Address: 192.168.197.35 Core-index 0 Current index 2 Index: 0 Time: 2015-10-16 20:37:34 Behavior: ONLINE Mac: 00d0.f822.33e7 Vid: 101 Port: Gi3/1 Timeused: 0d 00:00:00 Flow_up: 0 Flow_down: 0 Index: 1 Time: 2015-10-16 20:42:08 Behavior: OFFLINE Mac: 00d0.f822.33e7 Vid: 101 Port: Gi3/1 Timeused: 0d 00:04:27 Flow_up: 2107872 Flow_down: 2108224</pre> <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Index</td><td>The number of the record.</td></tr><tr><td>Time</td><td>Time when the record is made.</td></tr><tr><td>Behavior</td><td>Online or offline behavior.</td></tr><tr><td>MAC</td><td>The Mac address of a user.</td></tr><tr><td>Vid</td><td>The VLAN ID of a user.</td></tr><tr><td>Port</td><td>The user port.</td></tr><tr><td>Timeused</td><td>The time when a user gets online.</td></tr><tr><td>Flow UP</td><td>The uplink traffic of a user.</td></tr><tr><td>Flow down</td><td>The downlink traffic of a user.</td></tr></tbody></table>		Field	Description	Index	The number of the record.	Time	Time when the record is made.	Behavior	Online or offline behavior.	MAC	The Mac address of a user.	Vid	The VLAN ID of a user.	Port	The user port.	Timeused	The time when a user gets online.	Flow UP	The uplink traffic of a user.	Flow down	The downlink traffic of a user.
Field	Description																					
Index	The number of the record.																					
Time	Time when the record is made.																					
Behavior	Online or offline behavior.																					
MAC	The Mac address of a user.																					
Vid	The VLAN ID of a user.																					
Port	The user port.																					
Timeused	The time when a user gets online.																					
Flow UP	The uplink traffic of a user.																					
Flow down	The downlink traffic of a user.																					
Related Commands	Command	Description																				
	N/A	N/A																				
Platform Description	N/A																					

5.28 show web-auth template

	Use this command to display the portal server configuration.													
	show web-auth template													
Parameter Description	Parameter	Description												
	N/A	N/A												
Defaults	N/A													
Command Mode	Privileged EXEC mode													
Usage Guide	Use this command to display the portal server configuration.													
Configuration Examples	The following example displays the port server configuration. FS#show web-auth template Webauth Template Settings: ----- Name: eportalv1 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v1 ----- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-only-mode Type: v2 Port: 50100 Acctmlist: Authmlist: FS# <table><tr><th>Field</th><th>Description</th></tr><tr><td>Name</td><td>Template name.</td></tr><tr><td>Url</td><td>Server homepage address.</td></tr><tr><td>Ip</td><td>Server IP address.</td></tr><tr><td>Type</td><td>Server type, including the first generation portal server v1, the second generation portal server v2, and internal is intra.</td></tr><tr><td>Port</td><td>The protocol packet communication port of the server, which is on only the second generation portal server.</td></tr></table>		Field	Description	Name	Template name.	Url	Server homepage address.	Ip	Server IP address.	Type	Server type, including the first generation portal server v1, the second generation portal server v2, and internal is intra.	Port	The protocol packet communication port of the server, which is on only the second generation portal server.
Field	Description													
Name	Template name.													
Url	Server homepage address.													
Ip	Server IP address.													
Type	Server type, including the first generation portal server v1, the second generation portal server v2, and internal is intra.													
Port	The protocol packet communication port of the server, which is on only the second generation portal server.													

	Acctmlist	Accounting method list name, which is on the second generation portal and internal servers.
	Authmlist	Authentication method list name. which is on only the second generation portal and internal servers.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.29 show web-auth user

	Use this comma to display the online information, including IP address, interface, and online duration, of all users or the specified users.	
	show web-auth user { all ip ip-address mac mac-address name name-string }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address of the user.
	<i>mac-address</i>	MAC address of the user.
	<i>name-string</i>	User name.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the global Web authentication configuration and statistics. <pre> FS# show web-auth user all Current user num : 4, online 2 Address Online Time Limit Time Used Status Name ----- 192.168.0.11 On 0d 01:00:00 0d 00:15:10 Active 192.168.0.13 On 0d 01:00:00 0d 00:00:59 Active 111 192.168.0.25 Off 0d 01:00:00 0d 00:00:59 Create 192.168.0.46 Off 0d 01:00:00 0d 01:00:00 Destroy 222 FS# show web-auth user ip 192.168.0.11 Address : 192.168.0.11 </pre>	

	Mac : 00d0.f800.2233	
	Port : Gi0/2	
	Online : On	
	Time Limit : 0d 01:00:00	
	Time Used : 0d 00:15:10	
	Time Start : 2009-02-22 20:05:10	
	Status : Active	
	Field	Description
	Address	IP address of the user
	Mac	MAC address of the user
	Port	Access device port connected to the user
	Online	Whether the user is online
	Time Limit	Available duration of the user. 0 means unlimited.
	Time Used	Online duration of the user
	Time Start	Time when the user passes authentication and gets online
	Status	User status. Active means the user is normally online, Create means the user is created without any settings, Destroy means the user is deleted with its settings not cleared.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.30 url

	Use this command to set the portal server URL. Use the no form of this command to restore the default setting.	
	url <i>url-string</i>	
	no url	
Parameter Description	Parameter	Description
	<i>url-string</i>	Portal server URL, starting with http:// or https:// . The maximum length of this address is 255 bytes.
Defaults	On the first/second/inner/wifidog auth, no portal server URL is set by default. On WeChat auth, the URL when MCP/WMC server adopts WeChat and MSG auth by default.	
Command Mode	Template configuration mode	

Usage Guide	This command takes place of the http redirect homepage [<i>url-string</i>] command, which is now hidden as a compatible command., If no URL is specified, the default URL in the http://[ip-address] format will be adopted, among which ip-address is the IP address of the server.	
Configuration Examples	The following example sets the eportalv1 template URL to http://www.web-auth.net/login. <pre>FS(config.tmplt.eportalv1)#url http://www.web-auth.net/login</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.31 web-auth acl

	The whitelist users can access partial network resources before auth, and the blacklist users can not access partial network resources after auth. Use no form of this command to restore the default setting. web-auth acl {white-url name} no web-auth acl { white-url name}	
Parameter Description	Parameter	Description
	name	Whitelist URL
Command Mode	Global configuration mode	
Usage Guide	The command is used to check the whitelist configuration of web authentication.	
Configuration Examples	The following example configures whitelist. <pre>FS (config)# web-auth acl white-url www.FS.com.cn</pre>	
Platform Description	N/A	

5.32 web-auth dhcp-check

	Use this command to enable DHCP IP address check. Use no form of this command to restore the default setting.
	web-auth dhcp-check
	no web-auth dhcp-check

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	DHCP IP address check is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Only users whose IP addresses are allocated by DHCP are allowed to take authentication.	
Configuration Examples	The following example enables DHCP IP address check. <pre>FS (config)# web-auth dhcp-check</pre>	
Platform Description	N/A	

5.33 web-auth dhcp-check vlan

	Use this command to check whether the IP address of a client is assigned by the DHCP server. Use the no form of this command to restore the default setting.	
	web-auth dhcp-check {vlan [vlan-list]}	
	no web-auth dhcp-check	
Parameter Description	Parameter	Description
	vlan-list	Indicates the VLAN range in which DHCP address check needs to be enabled in interface.
Defaults	By default, this function is disabled.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example checks whether the IP address of a client is assigned by the DHCP server. <pre>FS(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan 1,3-4</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	

Description	

5.34 web-auth dhcp-server check

	Use this command to disable DHCP server detection.	
	no web-auth dhcp-server check	
	Use this form of this command to restore the default setting.	
	web-auth dhcp-server check	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, this function is enabled.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example disables DHCP server detection. FS (config)# no web-auth dhcp-server check	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.35 web-auth direct-host

	Use this command to set the authentication-exempted IP/MAC address range.	
	Use the no form of this command to restore the default setting.	
	web-auth direct-host { <i>ipv4-address</i> [<i>ip-mask</i>] [arp] <i>ipv6-address</i> } [port <i>interface-name</i>]	
	no web-auth direct-host { <i>ipv4-address</i> [<i>ip-mask</i>] <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	<i>ip-address</i>	IPv4 address of authentication-exempted user
	<i>ip-mask</i>	Mask of the IPv4 address free of authentication (optional).
	port <i>interface-name</i>	Binds user's IP address with a port of the access device (optional).
	arp	If ARP CHECK is enabled on the access device, keyword arp is needed for ARP

		binding of the IP address used by users free of authentication (optional). It is necessary for IPv4 addresses only.
Defaults	No user is exempted from authentication. All users must pass the Web authentication to access the restricted network resources.	
Command Mode	Global configuration mode	
Usage Guide	When a user is set to be exempted from authentication, it can access all reachable network resources without Web authentication. Up to 50 users can be set to be exempted from authentication.	
Configuration Examples	The following example sets the user with the IP address 172.16.0.1 to be exempted from authentication. FS(config)# web-auth direct-host 172.16.0.1 The following example sets the user with the IP address FF02::/64 to be exempted from authentication. FS(config)# web-auth direct-host FF02::/64	
Related Commands	Command	Description
	show web-auth direct-host	Displays the users free of Web authentication.
Platform Description	N/A	

5.36 web-auth enable

	Use this command to enable the Web authentication function on a port. This command is compatible with the web-auth port-control command.	
	Use the no form of this command to restore the default setting.	
	web-auth enable [eportalv1 eportalv2 <i>template-name</i>]	
	no web-auth enable	
Parameter Description	Parameter	Description
	eportalv1	Applies the first generation authentication template.
	eportalv2	Applies the second generation authentication template.
	<i>template-name</i>	Customized template.
Defaults	The Web authentication function is disabled on the port by default. The default template is eportalv1.	
Command	Interface configuration mode	

Mode		
Usage Guide	To ensure the Web authentication function, the authentication page URL should be configured. Because template applications are integrated into the controlled switch, the template or the server applications of the interface where the Web authentication function is disabled will be automatically cleared. This command is compatible with the original command that used to apply the template or server application in the global configuration mode.	
Configuration Examples	The following example enables the Web authentication function on gigabitEthernet 0/14. <pre>FS(config)# interface GigabitEthernet 0/14 FS(config-if-GigabitEthernet 0/14)# web-auth enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.37 web-auth linkdown-timeout

	Use this command to set the link-down timeout. Use the no form of this command to restore the default setting.	
	web-auth linkdown-timeout { <i>timeout</i> }	
	no web-auth linkdown-timeout	
Parameter Description	Parameter	Description
	<i>timeout</i>	Link-down timeout
Defaults	By default, the timeout is 60 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the link-down timeout to 30 seconds. <pre>FS (config)# web-auth linkdown-timeout 30</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

5.38 web-auth logging enable

	Use this command to enable the Web authentication syslog function. Use the no form of this command to restore the default setting.	
	web-auth logging enable { <i>num</i> }	
	no web-auth logging enable	
Parameter Description	Parameter	Description
	<i>num</i>	The syslog printing rate, indicating how many syslog entries can be printed in a second. The value is in the range from 0 to 65535. 0 indicates no limit.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to limit the syslog printing rate for only the functional module.	
Configuration Examples	The following example enables the syslog printing with no rate limit. <pre>FS(config)# web-auth logging enable 0</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

5.39 web-auth portal

	Use this command to map different portal servers with users in different subnets. Use the no form of this command to restore the default setting.	
	web-auth portal { <i>eportalv1</i> <i>eportalv2</i> } <i>name</i> }	
	no web-auth portal { <i>eportalv1</i> <i>eportalv2</i> } <i>name</i> }	
Parameter Description	Parameter	Description
	<i>name</i>	Portal server name
Defaults	This function is disabled by default.	

Command Mode	Global configuration mode
Usage Guide	N/A
Configuration Examples	N/A
Platform Description	N/A

5.40 web-auth portal extension

	Use this command to enable portal extension to support CMCC portal server. Use the no form of this command to restore the default setting. web-auth portal extension	
	no web-auth portal extension	
	default web-auth portal extension	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	By default, FS portal server is supported.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example disables portal extension. FS (config)# no web-auth portal extension	
Platform Description	N/A	

5.41 web-auth portal key

	Use this command to set the communication key between the access device and the authentication server. Use the no form of this command to clear the communication key between the redirected Web request of a user and the authentication server.
	web-auth portal key <i>key-string</i>
	no web-auth portal key

Parameter Description	Parameter	Description
	<i>key-string</i>	Communication key between the access device and the authentication server. The maximum length of the key is 255 bytes.
Defaults	No key is set by default.	
Command Mode	Global configuration mode	
Usage Guide	To use the Web authentication function, the communication key between the access device and the authentication server must be set.	
Configuration Examples	The following example sets the communication key between the access device and the authentication server to web-auth. <pre>FS(config)# web-auth portal key web-auth</pre>	
Related Commands	Command	Description
	http redirect	Sets the IP address of the authentication server.
	http redirect homepage	Sets the address of the authentication homepage.
	web-auth port-control	Enables the Web authentication on the port.
Platform Description	N/A	

5.42 web-auth portal-check

	Use this command to enable portal server check. Use the no form of this command to restore the default setting.	
	web-auth portal-check [interval <i>intsec</i>] [timeout <i>tosec</i>] [retransmit <i>retires</i>]	
	no web-auth porta-check	
Parameter Description	Parameter	Description
	<i>Intsec</i>	Check interval in the range from 1 to 1,000 in the unit of seconds. The default is 10 seconds.
	<i>tosec</i>	Timeout interval in the range from 1 to 1,000 in the unit of seconds. The default is 5 seconds.
	<i>retries</i>	Retry count in the range from 1 to 100. The default is 3.
Defaults	Portal server check is disabled by default.	

Command Mode	Global configuration mode
Usage Guide	It is recommended to use this command when there are multiple servers.
Configuration Examples	The following example enables portal server check. FS (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
Platform Description	N/A

5.43 web-auth portal-escape

	Use this command to enable portal-escape function. Use the no form of this command to restore the default setting.	
	web-auth portal-escape	
	no web-auth portal-escape	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command together with web-auth portal-check command to sustain key services when the portal server is abnormal.	
Configuration Examples	The following example enables portal-escape function. FS (config)# web-auth portal-escape	
Platform Description	N/A	

5.44 web-auth template

	Use this command to create the first generation authentication template and enter its configuration mode.
	web-auth template eportalv1
	Use this command to create the customized first generation authentication template and enter its configuration mode.
	web-auth template { template-name } v1

	Use this command to create the second generation authentication template and enter its configuration mode.	
	web-auth template eportalv2	
	Use this command to create the customized second generation authentication template and enter its configuration mode.	
	web-auth template { template-name } v2	
	Use this command to remove the template.	
	no web-auth template { template-name }	
Parameter Description	Parameter	Description
	eportalv1	Applies the first generation authentication template.
	eportalv2	Applies the second generation authentication template.
	template-name	Sets the name of the customized authentication template.
Defaults	No template is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	You can enter the eportalv1 template mode to configure the IP address and URL instead of executing the http redirect and http redirect homepage commands. The http redirect and http redirect homepage commands are compatible on the device, which will be converted to this command. The original command portal-server is compatible on the device, which will be converted to this command. To ensure the Web authentication function, configure and apply a functional portal server. The eportalv1 template is applied by default. The IP address, the URL and the communication secret key of the eportalv1 template should be configured. If no URL format is specified, the default http://[ip-address] format will be adopted. The IP address of the portal server is the network resource exempted from authentication, so the unauthenticated user can access it. The device limits the uplink traffic that accesses the IP address to prevent attacks. The upper limit is proportionate to the number of the physical ports.	
Configuration Examples	The following example configures the eportalv1 template. <pre>FS(config)# web-auth template eportalv1 FS(config.tmplt.eportalv1)#</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.45 web-auth update-interval

	Use this command to set the interval at which the online user information is updated. Use the no form of this command to restore the default setting.	
	web-auth update-interval {seconds}	
	no web-auth update-interval	
Parameter Description	Parameter	Description
	seconds	Update interval in seconds, in the range from 30 to 3,600 in the unit of seconds.
Defaults	The default is 180 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the interval at which the online user information is updated to 60 seconds. FS(config)# web-auth update-interval 60	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

5.46 web-auth vlan-control

	Use this command to configure the authenticable VLAN list. Use the no form of this command to restore the default setting.	
	web-auth vlan-control vlan-list	
	no web-auth vlan-control	
Parameter Description	Parameter	Description
	vlan-list	Authenticable VLAN list
Defaults	The default is port-control authentication.	
Command Mode	Interface configuration mode	

Usage Guide	N/A
Configuration	Use this command to configure the authenticable VLAN list.
Examples	FS (config-if-GigabitEthernet 0/1)# web-auth vlan-control 1
Platform Description	N/A

6 SCC Commands

6.1 Identifier Description

The following is a list of command identifiers used in commands for reference:

Identifier	Description
vlanlist	Authentication-exemption VLAN list
interval	Authenticated-user online-status detection interval
threshold	The traffic threshold of authenticated-user online-status detection

6.2 authmanage user-escape

	Use this command to enable user escape. authmanage user-escape { enable time <i>time-value1</i> when authentication-time <i>time-value2</i> when timeout-ratio <i>ratio-number</i> life <i>life-value</i> }	
	Use this command to disable user escape. no authmanage user-escape { enable time when authentication-time when timeout-ratio life }	
Parameter Description	Parameter	Description
	<i>time-value1</i>	Indicates the escape duration, in the unit of minutes.
	<i>time-value2</i>	Indicates the authentication duration, in the unit of ms. When the value exceeds that of <i>time-value2</i> , part of users is allowed to escape for <i>time-value1</i> minutes.
	<i>ratio-number</i>	When the ratio of authenticated users exceeds the value of <i>ratio-number</i> , part of users is allowed to escape for <i>time-value1</i> minutes.
	<i>life-value</i>	Indicates the escape lifetime, in the unit of minute.
Defaults	<i>time-value1</i> : The value is 30 minutes by default and can be set to 10 minutes to 240 minutes. <i>time-value2</i> : The default value is 5,000, which indicates that part of users are allowed to escape when the average handling duration exceeds 5s. The value ranges from 1,000 to 10,000. <i>ratio-number</i> : The default value is 10, which indicates that the part of users are allowed to escape when the ratio of timeout authentication users exceed 10%. The value ranges from 1 to 100. <i>life-value</i> : The value is 30 minutes by default and can be set to 10 minutes to 240 minutes.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	User escape needs to be enabled only when the system is detected to fail timely authentication.	

Configuration Examples	The following example enables user escape in global configuration mode. <pre>FS(config)# authmanage user-escape enable</pre>
Verification	Run show authmanage user-escape to display user escape configuration.
Prompt Messages	N/A
Common Errors	N/A
Platforms	This command is supported only on switches.

6.3 direct-vlan

	Use this command to configure authentication-exemption VLANs. direct-vlan <i>vlanlist</i>	
	Use this command to delete the authentication-exemption VLAN configuration. no direct-vlan <i>vlanlist</i>	
Parameter Description	Parameter	Description
	<i>vlanlist</i>	VLAN list, which can be a VLAN or a group of VLANs.
Defaults	By default, no authentication-exemption VLANs are configured.	
Command Mode	Global/Interface configuration mode	
Default Level	14	
Usage Guide	You can use this command to configure authentication-exemption VLANs, so that users in specified VLANs can access the Internet without experiencing dot1x or Web authentication. In interface configuration mode, the command takes effect on users from authentication-exempted VLANs of the interface.	
Configuration Examples	The following example configures the VLAN2 as an authentication-exemption VLAN. <pre>FS(config)# direct-vlan 2</pre>	
Verification	Use the show direct-vlan command to display the authentication-exemption VLAN configuration.	
Prompt	N/A	

Messages	
Common Errors	N/A
Platforms	N/A

6.4 nac-author-user maximum

	Use this command to configure the limit on IPv4 user capacity on a port. nac-author-user maximum <i>max-user-num</i>	
	Use this command to remove the limit on the IPv4 user capacity on a port. no nac-author-user maximum	
Parameter Description	Parameter	Description
	<i>max-user-num</i>	Defines the maximum number of IPv4 access users. The range is from 1 to 1,024.
Defaults	By default, the number of IPv4 access users is not limited.	
Command Mode	Interface configuration mode	
Default Level	14	
Usage Guide	Use this command to configure the maximum number of IPv4 access users on a port.	
Configuration Examples	The following example restricts the maximum number of IPv4 users to 100 on interface Gi 0/1. <pre>FS(config)#int gigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)#nac-author-user maximum 100</pre>	
Verification	1. Use the show nac-author-user command to display the current and the maximum numbers of IPv4 access users on all ports. 2. Use the show nac-author-user interface <i>interface-name</i> command to display the current and the maximum numbers of IPv4 access users on the specified port.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.5 offline-detect interval threshold

	Use this command to configure user online-status detection, so that a user is disconnected when its traffic is lower than a specified threshold or is zero in a specified interval. offline-detect interval <i>interval</i> threshold <i>threshold</i>	
	Use this command to restore the default user online-status detection configuration. default offline-detect	
	Use this command to disable user online-status detection. no offline-detect	
Parameter Description	Parameter	Description
	<i>interval</i>	Indicates the interval of traffic detection (in minutes). The range is from 1 to 65,535 in minutes on a non-switch device or from 6 to 65,535 in minutes on a switch.
	<i>threshold</i>	Indicates the traffic threshold (in bytes). The range is from 0 to 4,294,967,294 in bytes. The value of 0 indicates that the user is disconnected when no traffic of the user is detected.
Defaults	By default, the detection interval is 8 hours and the traffic threshold is 0.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	You can use this command to configure user online-status detection to enable the device to disconnect the authenticated user whose traffic is lower than a specified value and end accounting process.	
Configuration Examples	The following example directly disconnects a user for the user's traffic is lower than 5 Kbytes within 5 minutes. FS(config)#offline-detect interval 5 threshold 5120	
Verification	Use the show running command to display the configuration of online-status detection for authenticated users.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

6.6 show direct-vlan

	Use this command to display the authentication-exemption VLAN configuration. show direct-vlan	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Command Mode	Privileged EXEC mode	
Level	14	
Usage Guide	N/A	
Configuration Examples	The following example displays the authentication-exemption VLAN configuration. <pre>FS #show direct-vlan direct-vlan 5,7,100</pre>	
Prompt Messages	N/A	
Platforms	N/A	

6.7 show nac-author-user interface

	Use this command to display the capacity limit and current number of IPv4 users on all interfaces or a specified interface. show nac-author-user [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	<i>interface-name</i>	Interface name
Command Mode	Privileged EXEC mode	
Level	14	
Usage Guide	N/A	
Configuration Examples	The following example displays the current number and capacity limit of IPv4 users on interface Gi 0/1. <pre>FS#show nac-author-user interface gi 0/1</pre>	

	<table><tr><th>Port</th><th>Cur_num</th><th>Max_num</th></tr><tr><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>Gi0/1</td><td>0</td><td>100</td></tr></table>	Port	Cur_num	Max_num	-----	-----	-----	Gi0/1	0	100
Port	Cur_num	Max_num								
-----	-----	-----								
Gi0/1	0	100								
Prompt Messages	N/A									
Platforms	N/A									

6.8 station-move permit

	Use this command to enable authenticated-user migration. station-move permit	
	Use this command to disable authenticated-user migration. no station-move permit	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Authenticated-user migration is not permitted by default.	
Command Mode	Global configuration mode	
Level	14	
Usage Guide	You can enable the authenticated-user migration function to allow the online users to be authenticated again and get online from different physical locations (different ports or VLANs).	
Configuration Examples	The following examples enables authenticated-user migration. FS(config)#station-move permit	
Verification	Use the show running command to check whether the authenticated-user migration function is enabled.	
Prompt Messages	N/A	
Common Errors	N/A	
Platforms	N/A	

7 Global IP-MAC Binding Commands

7.1 address-bind

	Use this command to configure global IP-MAC address binding. Use the no form of this command to restore the default setting.	
	address-bind { <i>ip-address</i> <i>ipv6-address</i> } <i>mac-address</i>	
	no address-bind { <i>ip-address</i> <i>ipv6-address</i> } <i>mac-address</i>	
Parameter	Parameter	Description
Description	<i>ip-address</i>	IPv4 address to be bound
	<i>ipv6-address</i>	IPv6 address to be bound
	<i>mac-address</i>	MAC address to be bound
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example configures global IP-MAC address binding. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind 192.168.5.1 00d0.f800.0001</pre>	
Related Commands	Command	Description
	show address-bind	Displays the IP address-MAC address binding table.
Platform Description	N/A	

7.2 address-bind install

	Use this command to enable a binding policy globally. Use the no form of this command to restore the default setting.	
	address-bind install	
	no address-bind install	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	

Command Mode	Global configuration mode					
Usage Guide	If you bind an IP address to a MAC address, run this command to make the installation policy take effect.					
Configuration Examples	The following example enables a binding policy. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind 192.168.5.1 00d0.f800.0001 FS(config)# address-bind install</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>N/A</td><td>N/A</td></tr></table>	Command	Description	N/A	N/A	
Command	Description					
N/A	N/A					
Platform Description	N/A					

7.3 address-bind ipv6-mode

	This command is used to set the IPv6 address binding mode. Use the no form of this command to restore the default setting. This command is also used to set the compatible mode.	
	address-bind ipv6-mode { compatible loose strict }	
	no address-bind ipv6-mode	
Parameter	Parameter	Description
Description	compatible	Compatible mode
	loose	Loose mode
	strict	Strict mode
Defaults	The default is strict mode.	
Command Mode	Global configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example configures the IPv6 address binding mode. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind ipv6-mode compatible</pre>	

Related Commands	Command	Description
	show address-bind uplink	Displays the exceptional port of the address binding.
Platform Description	N/A	

7.4 address-bind uplink

	This command is used to configure the exception port. Use the no form of this command to restore the default setting.	
	address-bind uplink <i>interface-id</i>	
	no address-bind uplink <i>interface-id</i>	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Switching port or layer 2 aggregate port.
Defaults	All ports are non-exception ports by default.	
Command Mode	Global configuration mode.	
Usage Guide	If you have bound an IP address and a MAC address, the switch will discard the packets that have the same source IP address but different source MAC address. If the port is an exceptional port and is installed (see address-bind install), this binding policy does not take effect.	
Configuration Examples	The following example configures the exception port. <pre>FS# configure terminal Enter configuration commands, one per line. End with CNTL/Z. FS(config)# address-bind uplink GigabitEthernet 0/1</pre>	
Related Commands	Command	Description
	show address-bind uplink	Displays the exceptional port of address binding.
Platform Description	N/A	

7.5 show address-bind

	Use this command to display global IP address-MAC address binding.	
	show address-bind	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	N/A								
Command Mode	Privileged EXEC mode.								
Usage Guide	N/A								
Configuration Examples	The following example displays global IPv4 address-MAC address binding. <pre>FS#show address-bind Total Bind Addresses in System : 1 IP Address Binding MAC Addr ----- 192.168.5.1 00d0.f800.0001</pre> <table> <thead> <tr> <th>Field</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Total Bind Addresses in System</td><td>IPv4 address-MAC address binding count</td></tr> <tr> <td>IP Address</td><td>Bound IP address</td></tr> <tr> <td>Binding MAC Addr</td><td>Bound MAC address</td></tr> </tbody> </table>	Field	Description	Total Bind Addresses in System	IPv4 address-MAC address binding count	IP Address	Bound IP address	Binding MAC Addr	Bound MAC address
Field	Description								
Total Bind Addresses in System	IPv4 address-MAC address binding count								
IP Address	Bound IP address								
Binding MAC Addr	Bound MAC address								
Related Commands	<table> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>address-bind</td><td>Enables IP address-MAC address binding.</td></tr> </tbody> </table>	Command	Description	address-bind	Enables IP address-MAC address binding.				
Command	Description								
address-bind	Enables IP address-MAC address binding.								
Platform Description	N/A								

7.6 show address-bind uplink

	Use this command to display the exception port.	
	show address-bind uplink	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command mode	N/A	
Usage Guide	N/A	
Configuration Examples	The following example displays the exception port. <pre>FS#show address-bind uplink Port State ----- Gi0/1 Enabled</pre>	

	Default Disabled	
	Field	Description
	Port	Short for exception ports. All ports are non-exception ports by default.
	State	Indicates whether the port is exception port. State Enabled indicates that it is an exception port while state Disabled indicates that it is not.
Related Commands	Command	Description
	address-bind uplink	Sets the exception port.
Platform Description	N/A	

8 Password-Policy Commands

8.1 password policy life-cycle

	Use this command to set the password lifecycle. Use the no form of this command to restore the default setting.	
	password policy life-cycle <i>days</i>	
	no password policy life-cycle	
Parameter Description	Parameter	Description
	<i>days</i>	Sets the password lifecycle, in the range from 1 to 65,535 in the unit of days.
Defaults	No password lifecycle is set by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to set the password lifecycle. After the password lifecycle expires, the system reminds you to change the password when you login next time.  This function is valid for the global password (the enable password and the enable secret commands) and the local user password (the username <i>name</i> password <i>password</i> command) while not valid for the password in line mode.	
Configuration Examples	The following example sets the password lifecycle to 90 days. <pre>FS(config)# password policy life-cycle 90</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.2 password policy min-size

	Use this command to set the minimum length of the password. Use the no form of this command to restore the default setting.	
	password policy min-size <i>length</i>	
	no password policy min-size	

Parameter Description	Parameter	Description
	<i>length</i>	Sets the minimum length of the password, in the range from 1 to 31.
Defaults	No minimum length of the password is set by default.	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to set the minimum length of the password,  This function is valid for the global password (the <code>enable password</code> and the <code>enable secret</code> commands) and the local user password (the <code>username name password password</code> command) while not valid for the password in line mode.	
Configuration Examples	The following example sets the minimum length of the password to 8. <pre>FS(config)# password policy min-size 8</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.3 password policy no-repeat-times

	Use this command to ban the use of passwords used in the past several times. Use the <code>no</code> form of this command to restore the default setting.	
	password policy no-repeat-times <i>times</i>	
	no password policy no-repeat-times	
Parameter Description	Parameter	Description
	<i>times</i>	The past several times when passwords are configured, in the range from 1 to 31.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After this function is enabled, passwords used in the past several times are recorded. If the new password has been used, the alarm message is displayed and password configuration fails. This command is used to set the maximum number of password entries. When the actual number of password entries exceeds the configured number, the new password overwrites the oldest password.	

	 This function is valid for the global password (the <code>enable password</code> and the <code>enable secret</code> commands) and the local user password (the <code>username name password password</code> command) while not valid for the password in line mode.	
Configuration	The following example bans the use of passwords used in the past five times.	
Examples	FS(config)# password policy no-repeat-times 5	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

8.4 password policy strong

Use this command to enable strong password check.

password policy strong

no password policy strong

Parameter Description

Parameter	Description
N/A	N/A

Defaults

This function is disabled by default.

Command Mode

Global configuration mode

Usage Guide

If the following two kinds of passwords are set not matching the strength policy, the alarm message is displayed.

1. The password the same as the username.
2. The simple password containing only characters or numbers.

 This function is valid for the global password (the `enable password` and the `enable secret` commands) and the local user password (the `username name password password` command) while not valid for the password in line mode.

Configuration

The following example configures the strong password check.

Examples

FS(config)# password policy strong

Related Commands

Command	Description
N/A	N/A

Platform

N/A

Description

8.5 service password-encryption

	Use this command to encrypt a password. Use the no form of this command to restore default setting.	
	service password-encryption	
	no service password-encryption	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is disabled by default. Various passwords are displayed in plain text, unless they are encrypted. After you run the service password-encryption and show running or write command to save your configuration, the password changes into cipher text. If you disable the command, the password in cipher text cannot be restored to plain text.	
Configuration Examples	The following example encrypts the password: FS(config)# service password-encryption	
Related Commands	Command	Description
	enable password	Sets passwords of different privileges.
Platform Description	N/A	

8.6 show password policy

	Use this command to display the password security policy set by the user.	
	show password policy	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	This command is used to display the password security policy set by the user.	
Configuration Examples	The following example displays the password security policy set by the user.	
	FS#show password policy	
	Global password policy configurations:	
	Password encryption: Enabled	
	Password strong-check: Enabled	
	Password min-size: Enabled (6 characters)	
	Password life-cycle: Enabled (90 days)	
	Password no-repeat-times: Enabled (max history record: 5)	
	Field	Description
	Password encryption	Whether to encrypt the password.
	Password strong-check	Whether to enable password strong-check.
	Password min-size	Whether to set the minimum length of the password.
	Password life-cycle	Whether to set the password lifecycle.
	Password no-repeat-times	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9 Port Security Commands

9.1 switchport port-security

	Use this command to configure port security and the way to deal with violation. Use the no form of this command to restore the default setting.	
	switchport port-security [violation { protect restrict shutdown }]	
	no switchport port-security [violation]	
Parameter Description	Parameter	Description
	protect	Discards the packets breaching security.
	restrict	Discards the packets breaching security and sends the Trap message.
	shutdown	Discards the packets breaching the security, sends the Trap message and disables the interface.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	With port security, you can strictly control the input on a specific port by restricting access to the MAC address and IP address (optional) of the port on the switch. After you configure some secure addresses for the port security-enabled port, only the packets from these addresses can be forwarded. In addition, you can also restrict the maximum number of secure addresses on a port. If you set the maximum value to 1 and configure one secure address for this port, the workstation (whose address is the configured secure Mac address) connected to this port will occupy all the bandwidth of this port exclusively.  If the violation handling mode is changed after violation occurs, the new mode takes effect only after the violation mode is restarted.	
Configuration Examples	The following example enables port security on interface gigabitethernet 1/1, and the way to deal with violation is shutdown: <pre>FS(config)#interface gigabitethernet 1/1 FS(config-if)# switchport port-security FS(config-if)# switchport port-security violation shutdown</pre>	
Related Commands	Command	Description
	show port-security	Displays port security settings.
Platform Description	N/A	

9.2 switchport port-security aging

	Use this command to set the aging time for all secure addresses on an interface. Use the no form of this command to restore the default setting.	
	switchport port-security aging {static time time }	
	no switchport port-security aging {static time }	
Parameter Description	Parameter	Description
	static	Applies the aging time to both manually configured secure addresses and automatically learned addresses. Otherwise, apply it to only the automatically learned secure addresses.
	time time	Specifies the aging time for the secure address on this port. Its range is 0-1,440 in minutes. If you set it to 0, the aging function is disabled actually.
Defaults	No secure address is aged by default.	
Command Mode	Interface configuration mode	
Usage Guide	In interface configuration mode, use the no switchport port-security aging time command to disable the aging for security addresses on the port. Use the no switchport port-security aging static command to apply the aging time to only the dynamically learned security address. Use the show port-security command to display configuration. When both port security and 802.1X authentication functions are enabled, 802.1X clients must get re-authenticated for network access once the secure addresses are aged.  To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the switch automatically add or delete the secure addresses on the interface.	
Configuration Examples	The following example sets the aging time for all secure addresses on interface gigabitethernet 1/1 to eight minutes. <pre> FS# configure terminal FS(config)# interface gigabitethernet 1/1 FS(config-if)# switchport port-security aging time 8 FS(config-if)# switchport port-security aging static FS(config-if)# end </pre>	
Related Commands	Command	Description
	show port-security	Displays port security settings.
Platform Description	N/A	

9.3 switchport port-security binding

	Use these commands to configure secure address binding manually in the interface configuration mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the no form of these commands to remove the binding addresses.	
	switchport port-security binding [<i>mac-address</i> vlan <i>vlan_id</i>] { <i>ipv4-address</i> <i>ipv6-address</i> }	
	switchport port-security binding { <i>ipv4-address</i> <i>ipv6-address</i> }	
	no switchport port-security binding [<i>mac-address</i> vlan <i>vlan_id</i>] { <i>ipv4-address</i> <i>ipv6-address</i> }	
	no switchport port-security binding { <i>ipv4-address</i> <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	<i>mac-address</i>	The source MAC addresses to be bound
	<i>vlan_id</i>	VLAN ID of the binding source MAC address
	<i>ipv4-address</i>	Binds IPv4 addresses.
	<i>ipv6-address</i>	Binds IPv6 addresses.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	1. For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses. 2. For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.  Network is often accessible to static users with secure addresses without authorization. If authorization is configured, these users must comply with it.	
Configuration Examples	The following example binds the IP address 192.168.1.100 on interface g 0/10: <pre>FS# configure terminal FS(config)#interface gigabitethernet 0/10 FS(config-if)# switchport port-security binding 192.168.1.100 FS(config-if)# end</pre> The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on interface g 0/10. <pre>FS# configure terminal FS(config)#interface gigabitethernet 0/10 FS(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1 192.168.1.100 FS(config-if)# end</pre>	

Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding interface	Configures the secure address binding in privileged EXEC mode.
	switchport port-security mac-address	Sets the static secure address.
	switchport port-security aging	Sets the aging time for secure address.
Platform Description	N/A	

9.4 switchport port-security binding-filter logging

	Use this command to enable binding filter logging. Use the no form of these commands to restore the default setting.	
	switchport port-security binding-filter logging [rate-limit rate]	
	no switchport port-security binding-filter logging	
Parameter Description	Parameter	Description
	rate-limit rate	Indicates the printing rate of binding filter logging. The default rate is 10logs/minute. The configurable range is from 1 to 120 logs per minute.
Defaults	By default, binding filter logging is disabled.	
Command Mode	Global configuration mode	
Usage Guide	1. If you run the switchport port-security binding-filter logging command without configuring the <i>rate</i> parameter, binding filter logging is enabled and the default printing rate, 10logs/minute, is adopted. 2. After binding filter logging is enabled, for packets that do not comply with IP/IP-MAC binding, warnings are printed. 3. After binding filter logging is enabled, if the printing rate exceeds the configured rate, the number of suppressed packets is displayed.	
Configuration Examples	The following example enables binding filter logging. <pre>FS# configure terminal FS(config)# switchport port-security binding-filter logging FS(config)# end</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

9.5 switchport port-security interface binding

	Use these commands to configure secure address binding manually in the privileged EXEC mode through performing the source IP address plus source MAC address binding or only the source IP address binding. With this binding configured, only the packets match the binding secure address could enter the switch, others will be discarded. Use the no form of these commands to remove the binding addresses.	
	switchport port-security interface <i>interface-id</i> binding [<i>mac-address</i> vlan <i>vlan_id</i>] { <i>ipv4-address</i> <i>ipv6-address</i> }	
	switchport port-security interface <i>interface-id</i> binding { <i>ipv4-address</i> <i>ipv6-address</i> }	
	no switchport port-security interface <i>interface-id</i> binding [<i>mac-address</i> vlan <i>vlan_id</i>] { <i>ipv4-address</i> <i>ipv6-address</i> }	
	no switchport port-security interface <i>interface-id</i> binding { <i>ipv4-address</i> <i>ipv6-address</i> }	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Binds interface ID.
	<i>mac-address</i>	Binds source MAC address.
	<i>vlan_id</i>	VLAN ID of the binding source MAC address
	<i>ipv4-address</i>	Binds IPv4 address.
	<i>ipv6-address</i>	Binds IPv6 address .
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	- For packets complying with IP/IP-MAC binding, they can be forwarded only if MAC addresses are secure addresses. - For dynamic secure addresses, packets cannot be forwarded before bound even if their addresses comply with the binding list.	
Configuration Examples	The following example binds the IP address 192.168.1.100 on the interface g 0/10. <pre>FS# configure terminal FS(config)# switchport port-security binding interface g0/10 binding 192.168.1.100 FS(config)# end</pre>	

	The following example binds the IP address 192.168.1.100 and MAC address 00d0.f800.5555 with VLAN ID 1 on the interface g 0/10. <pre>FS# configure terminal FS(config)# switchport port-security binding interface g0/10 binding 00d0.f800.5555 vlan 1 192.168.1.100 FS(config)# end</pre>	
Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding in interface configuration mode.
	switchport port-security mac-address	Sets the static secure address.
	switchport port-security aging	Sets the aging time for secure address.
Platform Description	N/A	

9.6 switchport port-security mac-address

	Use this command to configure the static secure address. Use the no form of this command to remove the configuration.	
	switchport port-security mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]	
	no switchport port-security mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	<i>mac-address</i>	Static secure MAC address
	<i>vlan-id</i>	VLAN ID of the MAC address  The configuration of <i>vlan-id</i> is only supported on the TRUNK port.
Defaults	N/A	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively. <pre>FS# configure terminal FS(config)# interface gigabitethernet 0/10</pre>	

	<pre>FS(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2 FS(config-if)# end</pre>	
Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding.
	switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
	switchport port-security aging	Sets the aging time for the secure address.
Platform Description	N/A	

9.7 switchport port-security interface mac-address

	Use this command to configure the static secure address. Use the no form of this command to remove the configuration.	
	switchport port-security interface <i>interface-id</i> mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]	
	no switchport port-security interface <i>interface-id</i> mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]	
Parameter Description	Parameter	Description
	<i>interface-id</i>	Interface ID
	<i>mac-address</i>	Static secure address
	<i>vlan-id</i>	VLAN ID of the MAC address
	 The configuration of vlan-id is only supported on the TRUNK port.	
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the static secure address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 and 2 respectively. <pre>FS# configure terminal FS(config)# switchport port-security interface g0/10 mac-address 00d0.f800.5555 vlan 2 FS(config)# end</pre>	

Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding.
	switchport port-security mac-address	Sets the static secure address in interface configuration mode.
	switchport port-security aging	Sets the aging time for the secure address.
Platform Description	N/A	

9.8 switchport port-security maximum

	Use this command to set the maximum number of port secure addresses. Use the no form of this command to restore the default setting.	
	switchport port-security maximum <i>value</i>	
	no switchport port-security maximum	
Parameter Description	Parameter	Description
	<i>value</i>	Maximum number of the secure address, in the range from 1 to 128.
Defaults	The default is 128.	
Command Mode	Interface configuration mode	
Usage Guide	The number of the secure address contains the sum of static secure address and dynamically learnt secure address, 128 by default. If the number of the secure address you set is less than current number, it will prompt this setting failure.	
Configuration Examples	The following example sets the maximum number of the secure address to 2 for interface g 0/10. <pre> FS# configure terminal FS(config)#interface gigabitethernet 0/10 FS(config-if)# switchport port-security maximum 2 FS(config-if)# end </pre>	
Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding.
	Switchport port-security mac-address	Sets the static secure address in the interface

		configuration mode.
	switchport port-security aging	Sets the aging time for the port secure address.
Platform	N/A	
Description		

9.9 switchport port-security mac-address sticky

	Use this command to configure the Sticky MAC secure address. Use the no form of this command to restore the default setting.	
	switchport port-security mac-address sticky <i>mac-address</i> [vlan <i>vlan-id</i>]	
	no switchport port-security mac-address sticky <i>mac-address</i> [vlan <i>vlan-id</i>]	
	Use the command without parameters to enable the Sticky MAC address learning. Use the no form of this command to disable the Sticky MAC address learning.	
	switchport port-security mac-address sticky	
	no switchport port-security mac-address sticky	
Parameter Description	Parameter	Description
	<i>mac-address</i>	Static secure address
	<i>vlan-id</i>	Vlan ID of the MAC address
		 The configuration of <i>vlan-id</i> is only supported on the TRUNK port.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Sticky MAC addresses, either static or dynamic, are special addresses free from aging.	
Configuration Examples	The following example sets the MAC address and VLAN ID of TRUNK port 10 to 00d0.f800.5555 to 2 respectively. <pre> FS# configure terminal FS(config)#interface gigabitethernet 0/10 FS(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2 FS(config-if)# end </pre> The following example enables the Sticky MAC address learning on interface g0/10. <pre> FS# configure terminal FS(config)#interface gigabitethernet 0/10 FS(config-if)# switchport port-security sticky mac-address FS(config-if)# end </pre>	

Related Commands	Command	Description
	show port-security	Displays port security settings.
	switchport port-security	Enables the port-security.
	switchport port-security binding	Configures the secure address binding.
	switchport port-security mac-address interface	Sets the static secure address in privileged EXEC mode.
	switchport port-security mac-address	Sets the static secure address in interface configuration mode.
	switchport port-security aging	Sets the aging time for the secure address.
Platform Description	N/A	

9.10 show port-security

	Use this command to display the port security configuration and the secure address.	
	show port-security [address [interface <i>interface-id</i>] binding [interface <i>interface-id</i>] interface <i>interface-id</i> all]	
Parameter Description	Parameter	Description
	address	Displays all secure addresses, or the secure address of the specified port.
	binding	Displays all port security bindings, or the port security bindings of the specified port.
	interface <i>interface-id</i>	Displays the port security configuration of the specified port.
	all	Displays all valid secure addresses and valid port security bindings.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	To display all port security configuration and violation management, execute the command without any parameter. To display the security configuration, the secure address, or the port security binding of the specified interface, execute the command with the corresponding parameter.	
Configuration Examples	The following example displays the port security statistics. <pre> FS#show port-security NO. SecurePort MaxSecureAddr CurrentAddr CurrentIpBind CurrentIpMacBind SecurityAction (Count) (Count) (Count) (Count) ----- 1 Gi0/1 128 2 2 1 protect ----- Total secure addresses in System : 2 </pre>	

Total secure bindings in System : 3

Field	Description
NO.	Serial number.
Secure Port	Port name
MaxSecureAddr(count)	The maximum number of secure addresses on the port.
CurrentAddr(count)	The current number of secure addresses on the port.
CurrentIpBind (count)	The current number of IP addresses bindings on the port.
CurrentIpMacBind (count)	The current number of IP-MAC address bindings on the port.
Security Action	Violation management.
Total secure addresses in System	The total number of secure addresses on the device.
Total secure bindings in System	The total number of port security bindings on the device,

The following example displays the port security configuration on interface GigabitEthernet 0/1.

FS#show port-security interface gigabitEthernet 0/1

```

Interface           : GigabitEthernet 0/1
Port status         : down
Port Security       : enabled
SecureStatic address aging : disabled
Sticky dynamic address : disabled
Violation mode      : protect
Maximum MAC Addresses : 128
Total MAC Addresses : 2
Configured MAC Addresses : 2
Dynamic MAC Addresses : 0
Sticky MAC Addresses : 0
Total security binding : 3
IPv4-ONLY Binding Addresses : 1
IPv6-ONLY Binding Addresses : 1
IPv4-MAC Binding Addresses : 1
IPv6-MAC Binding Addresses : 0
Aging time(min)     : 0
  
```

Field	Description
Interface	Port name.
Port status	Port status.
Port Security	Displays whether the port security is enabled.
SecureStatic address aging	Displays whether the static secure address aging is enabled.
Sticky dynamic address	Displays whether the dynamic secure address is converted to the sticky secure address,

Violation mode	Port violation management.
Maximum MAC Addresses	The maximum number of secure addresses on the port.
Total MAC Addresses	The number of valid secure addresses on the port.
Configured MAC Addresses	The number of static secure addresses.
Dynamic MAC Addresses	The number of dynamic secure addresses.
Sticky MAC Addresses	The number of sticky secure addresses.
Total security binding	The number of valid port security bindings.
IPv4-ONLY Binding Addresses	The number of IPv4 addresses bindings.
IPv6-ONLY Binding Addresses	The number of IPv6 addresses bindings.
IPv4-MAC Binding Addresses	The number of IPv4-MAC address bindings.
IPv6-MAC Binding Addresses	The number of IPv6-MAC address bindings.
Aging time(min)	The aging time of the secure address.

The following example displays all secure addresses on the device.

FS#show port-security address

NO.	VLAN	MacAddress	PORT	TYPE	RemainingAge(mins)	STATUS
1	1	00d0.f800.073c	GigabitEthernet 0/1	Configured	--	active
2	1	00d0.f800.073d	GigabitEthernet 0/1	Configured	--	active

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
Type	Secure address type.
Remaining Age(mins)	The aging time of the secure address.
STATUS	The secure address status.

The following example displays all port security bindings on the device.

FS#show port-security binding

NO.	VLAN	MacAddress	PORT	IpAddress	FilterType	FilterStatus
1	1	00d0.f800.073c	Gi0/1	192.168.12.202	ipv4-mac	active
2	--	--	Gi0/1	192.168.0.1	ipv4-only	active
3	--	--	Gi0/1	ffaa:ddcc::1	ipv6-only	activ

Field	Description
NO.	Serial number.
Vlan	VLAN ID.
Mac Address	MAC address.
Port	Port name.
IpAddress	IP address.
FilterType	The filtering type of the port security binding.

	FilterStatus	The status of the port security binding.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

10 Storm Control Commands

10.1 show storm-control

	Use this command to display storm suppression information.											
	show storm-control [<i>interface-type interface-number</i>]											
Parameter Description	Parameter	Description										
	<i>interface-type interface-number</i>	Specifies an interface.										
Defaults	N/A											
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode											
Usage Guide	N/A											
Configuration Examples	The following example displays storm control configuration on FastEthernet 0/1. <pre>FS# show storm-control fastEthernet 0/1</pre> <table><thead><tr><th>Interface</th><th>Broadcast Control</th><th>Multicast Control</th><th>Unicast Control</th><th>Action</th></tr></thead><tbody><tr><td>FastEthernet 0/1</td><td>1%</td><td>50%</td><td>1%</td><td>none</td></tr></tbody></table>		Interface	Broadcast Control	Multicast Control	Unicast Control	Action	FastEthernet 0/1	1%	50%	1%	none
Interface	Broadcast Control	Multicast Control	Unicast Control	Action								
FastEthernet 0/1	1%	50%	1%	none								
Related Commands	Command	Description										
	storm-control	Enables storm suppression.										
Platform Description	N/A											

10.2 storm-control

	Use this command to enable the storm suppression for unknown unicast packets. Use the no or default form of this command to restore the default setting.
	storm-control unicast [{ <i>level percent</i> <i>pps packets</i> <i>rate-bps</i> }]
	no storm-control unicast
	default storm-control unicast
	Use this command to enable the storm suppression for multicast packets. Use the no or default form of this command to restore the default setting.
	storm-control multicast [{ <i>level percent</i> <i>pps packets</i> <i>rate-bps</i> }]
	no storm-control multicast
	default storm-control multicast

	Use this command to enable the storm suppression for broadcast packets. Use the no or default form of this command to restore the default setting.	
	storm-control broadcast [{ level <i>percent</i> pps <i>packets</i> <i>rate-bps</i> }]	
	no storm-control broadcast	
	default storm-control broadcast	
Parameter Description	Parameter	Description
	level <i>percent</i>	Sets the bandwidth percentage, for example, 20 means 20%.
	pps <i>packets</i>	Sets the pps, which means packets per second.
	<i>rate-bps</i>	Rate allowed
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Too many broadcast, multicast or unicast packets received on a port may cause storm and thus slow network and increase timeout. Protocol stack implementation errors or wrong network configuration may also lead to such storms. A device can implement the storm suppression to a broadcast, a multicast, or a unicast storm respectively. When excessive broadcast, multicast or unknown unicast packets are received, the switch temporarily prohibits forwarding of relevant types of packets till data streams are recovered to the normal state (then packets will be forwarded normally).	
Configuration Examples	The following example enables the multicast storm suppression on FastEthernet 0/1 and sets the allowed rate to 4M. <pre>FS(config)# int fastEthernet 0/1 FS(config-if-FastEthernet 0/1)# storm-control multicast 4096</pre>	
Related Commands	Command	Description
	show storm-control	Displays storm suppression information.
Platform Description	N/A	

11 SSH Commands

11.1 crypto key generate

	Use this command to generate a public key to the SSH server.	
	crypto key generate { rsa dsa }	
Parameter	Parameter	Description
Description	rsa	Generates an RSA key.
	dsa	Generates a DSA key.
Defaults	By default, the SSH server does not generate a public key.	
Command Mode	Global configuration mode	
Usage Guide	When you need to enable the SSH SERVER service, use this command to generate a public key on the SSH server and enable the SSH SERVER service by command enable service ssh-server at the same time. SSH 1 uses the RSA key; SSH 2 uses the RSA or DSA key. Therefore, if a RSA key has been generated, both SSH1 and SSH2 can use it. If only a DSA key is generated, only SSH2 can use it.  Only DSA/RSA authentication is available for one connection. Also, the key algorithm may differ in different client. Thus, it is recommended to generate both RSA and DSA keys so as to ensure connection with the portal server.  RSA has a minimum modulus of 512 bits and a maximum modulus of 2,048 bits; DSA has a minimum modulus of 360 bits and a maximum modulus of 2,048 bits. For some clients like SCP clients, a 768-bit or more key is required. Thus, it is recommended to generate the key of 768 bits or more.  A key can be deleted by using the no crypto key generate command. The no crypto key zeroize command is not available.	
Configuration Examples	The following example generates an RSA key to the SSH server. <pre>FS# configure terminal FS(con fig)# crypto key generate rsa</pre>	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
	crypto key zeroize { rsa dsa }	Deletes DSA and RSA keys and disables the SSH server function.
Platform Description	N/A	

11.2 crypto key zeroize

	Use this command to delete a public key to the SSH server.	
	crypto key zeroize { rsa dsa }	
Parameter	Parameter	Description
Description	rsa	Deletes the RSA key.
	dsa	Deletes the DSA key.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command deletes the public key to the SSH server. After the key is deleted, the SSH server state becomes DISABLE. If you want to disable the SSH server, run the no enable service ssh-server command.	
Configuration Examples	The following example deletes a RSA key to the SSH server. FS# configure terminal FS(config)# crypto key zeroize rsa	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
	crypto key generate { rsa dsa }	Generates DSA and RSA keys.
Platform Description	N/A	

11.3 disconnect ssh

	Use this command to disconnect the established SSH connection.	
	disconnect ssh [vty] session-id	
Parameter	Parameter	Description
Description	vtty	Established VTY connection
	<i>session-id</i>	ID of the established SSH connection, in the range from 0 to 35
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	You can disconnect a SSH connection by entering the ID of the SSH connection or disconnect a SSH connection by entering the specified VTY connection ID. Only connections of the SSH type can be disconnected.	

Configuration Examples	The following example disconnects the established SSH connection by specifying the SSH session ID. <pre>FS# disconnect ssh 1</pre> The following example disconnects the established SSH connection by specifying the VTY session ID. <pre>FS# disconnect ssh vty 1</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ssh</td><td>Displays the information about the established SSH connection.</td></tr><tr><td>clear line vty <i>line_number</i></td><td>Disconnects the current VTY connection.</td></tr></table>	Command	Description	show ssh	Displays the information about the established SSH connection.	clear line vty <i>line_number</i>	Disconnects the current VTY connection.	
Command	Description							
show ssh	Displays the information about the established SSH connection.							
clear line vty <i>line_number</i>	Disconnects the current VTY connection.							
Platform Description	N/A							

11.4 ip scp server enable

	Use this command to enable the SCP server function on a network device.	
	Use the no form of this command to restore the default setting.	
	ip scp server enable	
	no ip scp server enable	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Secure Copy (SCP) enables an authenticated user to transfer files to/from a remote device in an encrypted way, with high security and guarantee.	
Configuration Examples	The following example enables the SCP server function. FS# configure terminal FS(config)# ip scp server enable	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
Platform Description	N/A	

11.5 ip scp server topdir

	Use this command to set the path for uploading/downloading files to/from the SCP server. Use the no form of this command to restore the default settings. ip scp server topdir {flash:/path flash2:/path usb0:/path usb1:/path sd0:/path sata0:/path tmp:/path }	
	no ip scp server topdir	
Parameter Description	Parameter	Description
	flash	Selects the file transfer path from the extended flash memory. The file transfer path is flash:/ by default.
	flash2	Selects the file transfer path from Extended Flash Memory 2. This option is supported only when the device has the data2 partition.
	usb0	Selects the file transfer path from USB Disk 0. This option is supported only when the device has one USB interface and is connected with an extended USB device.
	usb1	Selects the file transfer path from USB Disk 1. This option is supported only when the device has two USB interfaces and is connected with extended USB devices.
	sd0	Selects the file transfer path from the SD card. This option is supported only when the device has an SD card interface and is connected with an extended SD card.
	sata0	Selects the file transfer path from the hard disk. This option is supported only when the device has the SATA partition.
	tmp	Sets the file transfer path to tmp/vsd/ .
Defaults	The file transfer path is flash:/ by default.	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	This command is used to change the file transfer path for uploading and downloading files.	
Configuration Examples	The following example changes the file transfer path to tmp/vsd. <pre>FS# configure terminal FS(config)# ip scp server topdir tmp:/</pre>	

11.6 ip ssh access-class

	Use this command to set the ACL filtering of the SSH server.	
	ip ssh access-class { access-list-number access-list-name }	
	Use the no form of this command to delete the ACL filtering of the SSH server. no ip ssh access-class	
Parameter Description	Parameter	Description
	<i>access-list-number</i>	The ACL number and the number range is configurable. The standard ACL

		number ranges are 1 to 99 and 1,300 to 1,999. The extended ACL number ranges are 100 to 199 and 2,000 to 2,699.
	<i>access-list-name</i>	An ACL name.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Run this command to perform ACL filtering for all connections to the SSH server. In line mode, ACL filtering is performed only for specific lines. However, ACL filtering rules of the SSH are effective to all SSH connections.	
Configuration Examples	The following example performs the ACL filtering named testv4 for all connections to the SSH server. <pre>FS# configure terminal FS(config)# ip ssh access-class testv4</pre>	
Platform Description	N/A	

11.7 ip ssh authentication-retries

	Use this command to set the authentication retry times of the SSH server. Use the no form of this command to restore the default setting.	
	ip ssh authentication-retries <i>retry times</i>	
	no ip ssh authentication-retries	
Parameter Description	Parameter	Description
	<i>retry times</i>	Authentication retry times, ranging from 0 to 5
Defaults	The default is 3.	
Command Mode	Global configuration mode	
Usage Guide	User authentication is considered failed if authentication is not successful when the configured authentication retry times on the SSH server is exceeded. Use the show ip ssh command to display the configuration of the SSH server	
Configuration Examples	The following example sets the authentication retry times to 2. <pre>FS# configure terminal FS(config)# ip ssh authentication-retries 2</pre>	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.

Platform	N/A
Description	

11.8 ip ssh cipher-mode

	Use this command to set the SSH server encryption mode. Use the no form of this command to restore the default setting.	
	ip ssh cipher-mode { cbc ctr others }	
	no ip ssh cipher-mode	
Parameter Description	Parameter	Description
	cbc	Encryption mode: CBC (Cipher Block Chaining) Encryption algorithm: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blow fish-CBC
	ctr	Encryption mode: CTR (Counter) Encryption algorithm: AES128-CTR, AES192-CTR, AES256-CTR
	others	Encryption mode: Others Encryption algorithm: RC4
Defaults	All encryption modes are supported by default.	
Command Mode	Global configuration mode	
Usage Guide	This command is used to set the SSH server encryption mode. For FS Networks, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC; the SSHv2 server supports AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, and RC4. All these algorithms can be grouped into CBC, CTR and Other as shown above. With the advancement of cryptography study, CBC and Others encryption modes are proved to easily decipher. It is recommended to enable the CTR mode to raise assurance for organizations and enterprises demanding high security.	
Configuration Examples	The following example enables CTR encryption mode. <pre>FS# configure terminal FS(config)# ip ssh cipher-mode ctr</pre>	
Platform Description	N/A	

11.9 ip ssh hmac-algorithm

	Use this command to set the algorithm for message authentication . Use the no form of this command to restore the default setting.
	ip ssh hmac-algorithm { md5 md5-96 sha1 sha1-96 }
	no ip ssh hmac-algorithm

Parameter	Parameter	Description
Description	md5	MD5 algorithm
	md5-96	MD5-96 algorithm
	sha1	SHA1 algorithm
	sha1-96	SHA1-96 algorithm
Defaults	SSHv1: all the algorithms are not supported. SSHv2: all the algorithms are supported.	
Command Mode	Global configuration mode	
Usage Guide	FS SSHv1 servers do not support algorithms for message authentication . For FS Networks, the SSHv1 server does not support message authentication algorithms; the SSHv2 server supports MD5, MD5-96, SHA1, and SHA1-96 algorithms. Set the algorithm on your demand.	
Configuration Examples	The following example sets the algorithm for message authentication to SHA1. FS# configure terminal FS(config)# ip ssh hmac-algorithm sha1	
Platform Description	N/A	

11.10 ip ssh key-exchange

	Use this command to configure support for DH key exchange method on the SSH server Use the no form of this command to restore the default setting.	
	ip ssh key-exchange { dh_group_exchange_sha1 dh_group14_sha1 dh_group1_sha1 }	
	no ip ssh key-exchange	
Parameter Description	Parameter	Description
	dh_group_exchange_sha1	Indicates configuration of diffie-hellman-group-exchange-sha1 for keyexchange. The key has 2,048 bytes, which cannot be edited.
	dh_group14_sha1	Indicates configuration of diffie-hellman-group14-sha1 for keyexchange. The key has 2,048 bytes.
	dh_group1_sha1	Indicates configuration of diffie-hellman-group1-sha1 for keyexchange. The key has 1,024 bytes.
Defaults	By default, the SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1 and diffie-hellman-group14-sha1 for key exchange.	
Command Mode	Global configuration mode	
Usage Guide	N/A	

Configuration Examples	The following example configures the support for diffie-hellman-group14-sha1. <pre>FS# configure terminal FS(config)# ip ssh key-exchange dh_group14_sha1</pre>					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip ssh</td><td>Displays the current status of the SSH server.</td></tr></table>	Command	Description	show ip ssh	Displays the current status of the SSH server.	
Command	Description					
show ip ssh	Displays the current status of the SSH server.					
Platform Description	N/A					

11.11 ip ssh peer

	Use this command to associate the public key file and the user name on the client. During client login authentication, you can specify a public key file based on the user name. Use the no form of this command to restore the default setting.	
	ip ssh peer <i>username</i> public-key { rsa dsa } <i>filename</i>	
	no ip ssh peer <i>username</i> public-key { rsa dsa } <i>filename</i>	
Parameter	Parameter	Description
Description	<i>username</i>	User name
	<i>filename</i>	Name of a public key file
	rsa	The public key is a RSA key
	dsa	The public key is a DSA key
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets RSA and DSA key files associated with user test . FS# configure terminal FS(config)# ip ssh peer test public-key rsa flash:rsa.pub FS(config)# ip ssh peer test public-key dsa flash:dsa.pub	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
Platform Description	N/A	

11.12 ip ssh port

	Use this command to set a monitoring port ID for the SSH server. ip ssh port <i>port</i>	
	Use either of the following commands to restore the monitoring port ID of the SSH server to the default value. no ip ssh port ip ssh port 22	
Parameter	Parameter	Description
Description	<i>port</i>	Monitoring port ID of the SSH server. The value ranges from 1025 to 65535.
Defaults	N/A	
Command Mode	Global configuration mode	
Default Level	14	
Usage Guide	N/A	
Configuration Examples	The following example sets the monitoring port ID of the SSH server to 10000. <pre>FS# configure terminal FS(config)# ip ssh port 10000</pre>	
Verification	Run the show ip ssh command to display the configured monitoring port ID of the SSH server.	
Prompts	1. If the required port ID is the same as the current value, a prompt is displayed, indicating that the current port ID is the required value. <pre>FS(config)# ip ssh port 22 % SSH tcp-port has been 22</pre> 2. If a port in the monitoring state is configured as the monitoring port of the SSH server, a prompt is displayed, indicating that the port is already in the monitoring state and you are required to set another port ID, and the SSH server still uses the previous port ID. <pre>FS(config)# ip ssh port 10000 % SSH open tcp-port(10000) failed, please use another tcp-port, otherwise the system will use the old tcp-port(22)!</pre> 3. If a monitoring error occurs after a monitoring port ID is configured for the SSH server, a port ID configuration failure prompt is displayed. <pre>FS(config)# ip ssh port 10000 % SSH change to tcp-port(10000) fail!</pre> 4. If a port ID is configured successfully, a port ID configuration success prompt is displayed.	

```
FS(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

11.13 ip ssh time-out

	Use this command to set the authentication timeout for the SSH server. Use the no form of this command to restore the default setting.	
	ip ssh time-out <i>time</i>	
	no ip ssh time-out	
Parameter	Parameter	Description
Description	<i>time</i>	Authentication timeout, in the range from 1 to 120 in the unit of seconds
Defaults	The default is 120 seconds.	
Command Mode	Global configuration mode	
Usage Guide	The authentication is considered timeout and failed if the authentication is not successful within 120 seconds starting from receiving a connection request. Use the show ip ssh command to display the configuration of the SSH server.	
Configuration Examples	The following example sets the timeout value to 100 seconds. <pre>FS# configure terminal FS(config)# ip ssh time-out 100</pre>	
Related Commands	Command	Description
	show ip ssh	Displays the current status of the SSH server.
Platform Description	N/A	

11.14 ip ssh version

	Use this command to set the version of the SSH server. Use the no form of this command to restore the default setting.	
	ip ssh version { 1 2 }	
	no ip ssh version	
Parameter	Parameter	Description
Description	1	Supports the SSH1 client connection request.
	2	Supports the SSH2 client connection request.
Defaults	SSH1 and SSH2 are compatible by default.	

Command Mode	Global configuration mode					
Usage Guide	This command is used to configure the SSH connection protocol version supported by SSH server. By default, the SSH server supports SSH1 and SSH2. If Version 1 or 2 is set, only the SSH client of this version can connect to the SSH server. Use the show ip ssh command to display the current status of SSH server.					
Configuration Examples	The following example sets the version of the SSH server. FS# configure terminal FS(config)# ip ssh version 2					
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show ip ssh</td><td>Displays the current status of the SSH server.</td></tr></table>	Command	Description	show ip ssh	Displays the current status of the SSH server.	
Command	Description					
show ip ssh	Displays the current status of the SSH server.					
Platform Description	N/A					

11.15 ipv6 ssh access-class

	Use this command to set the IPv6 ACL filtering of the SSH server.	
	ipv6 ssh access-class <i>accessv6-list-name</i>	
	Use the no form of this command to delete the IPv6 ACL filtering of the SSH server.	
	no ipv6 ssh access-class	
Parameter Description	Parameter	Description
	<i>accessv6-list-name</i>	An IPv6 ACL name.
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Run this command to perform IPv6 ACL filtering for all connections to the SSH server. In line mode, IPv6 ACL filtering is performed only for specific lines. However, IPv6 ACL filtering rules of the SSH are effective to all SSH connections.	
Configuration Examples	The following example performs the IPv6 ACL filtering named testv6 for all connections to the SSH server. FS# configure terminal FS(config)# ipv6 ssh access-class testv6	
Platform	N/A	

Description	

11.16 show crypto key mypubkey

	Use this command to display the information about the public key part of the public key to the SSH server.	
	show crypto key mypubkey { rsa dsa }	
Parameter	Parameter	Description
Description	rsa	Displays the RSA key.
	dsa	Displays the DSA key.
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode	
Usage Guide	This command is used to show the information about the public key part of the generated public key on the SSH server, including key generation time, key name, contents in the public key part, etc.	
Configuration Examples	The following example displays the information about the public key part of the public key to the SSH server. <pre>FS(config)#show crypto key mypubkey rsa % Key pair was generated at: 7:1:25 UTC Jan 16 2013 Key name: RSA1 private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAEAA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q10kz+4/ /IgYR0ge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw== % Key pair was generated at: 7:1:25 UTC Jan 16 2013 Key name: RSA private Usage: SSH Purpose Key Key is not exportable. Key Data: AAAAAwEA AQAAAEAA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3 LEYYfQ9s pgYL0ZQf S0s/GY0X gJOMsc6z i8OAKQ==</pre>	
Related Commands	Command	Description
	crypto key generate { rsa dsa }	Generates DSA and RSA keys.
Platform Description	N/A	

11.17 show ip ssh

	Use this command to display the information of the SSH server.	
	show ip ssh	
Parameter	Parameter	Description
Description	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode/Global configuration mode	
Usage Guide	This command is used to display the information of the SSH server, including version, enablement state, port ID, encryption, message authentication algorithm, authentication timeout, and authentication retry times. Note: If no key is generated for the SSH server, the SSH version is still unavailable even if this SSH version has been configured.	
Configuration Examples	The following example displays the information of the SSH server. <pre> FS(config)#show ip ssh SSH Disable - version 1.99 please generate rsa and dsa key to enable SSH SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: disabled // 显示 SSH Server 功能和 SCP 功能均已打开的配置信息 FS(config)#show ip ssh SSH Enable - version 1.99 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1 Authentication timeout: 120 secs Authentication retries: 3 SSH SCP Server: enabled </pre>	
Related Commands	Command	Description
	ip ssh version {1 2}	Configures the version for the SSH server.
	ip ssh time-out time	Sets the authentication timeout for the SSH server.

	ip ssh authentication-retries	Sets the authentication retry times for the SSH server.
Platform	N/A	
Description		

11.18 show ssh

	Use this command to display the information about the established SSH connection.																																									
	show ssh																																									
Parameter	Parameter			Description																																						
Description	N/A			N/A																																						
Defaults	N/A																																									
Command Mode	Privileged EXEC mode/Global configuration mode																																									
Usage Guide	This command is used to display the information about the established SSH connection, including VTY number of connection, SSH version, encryption algorithm, message authentication algorithm, connection status, and user name.																																									
Configuration Examples	The following example displays the information about the established SSH connection: FS#show ssh <table><thead><tr><th>Connection</th><th>Version</th><th>Encryption</th><th>Hmac</th><th>Compress</th><th>State</th><th>Username</th></tr></thead><tbody><tr><td>0</td><td></td><td>1.5 blowfish</td><td></td><td>zlib</td><td>Session started</td><td>test</td></tr><tr><td>1</td><td></td><td>2.0 aes256-cbc</td><td>hmac-sha1</td><td>zlib</td><td>Session started</td><td>test</td></tr></tbody></table> Field Description <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Connection</td><td>VTY number</td></tr><tr><td>Version</td><td>SSH version</td></tr><tr><td>Encryption</td><td>Encryption algorithm</td></tr><tr><td>Hmac</td><td>Message authentication algorithm</td></tr><tr><td>Compress</td><td>Compress algorithm</td></tr><tr><td>State</td><td>Connection state</td></tr><tr><td>Username</td><td>Username</td></tr></tbody></table>					Connection	Version	Encryption	Hmac	Compress	State	Username	0		1.5 blowfish		zlib	Session started	test	1		2.0 aes256-cbc	hmac-sha1	zlib	Session started	test	Field	Description	Connection	VTY number	Version	SSH version	Encryption	Encryption algorithm	Hmac	Message authentication algorithm	Compress	Compress algorithm	State	Connection state	Username	Username
Connection	Version	Encryption	Hmac	Compress	State	Username																																				
0		1.5 blowfish		zlib	Session started	test																																				
1		2.0 aes256-cbc	hmac-sha1	zlib	Session started	test																																				
Field	Description																																									
Connection	VTY number																																									
Version	SSH version																																									
Encryption	Encryption algorithm																																									
Hmac	Message authentication algorithm																																									
Compress	Compress algorithm																																									
State	Connection state																																									
Username	Username																																									
Related Commands	Command			Description																																						
	N/A			N/A																																						
Platform Description	N/A																																									

12 URPF Commands

12.1 clear ip urpf

	Use this command to clear IPv4 URPF packet drop statistics.	
	clear ip urpf [interface <i>interface-name</i>]	
Parameter Description	Parameter	Description
	interface <i>interface-name</i>	Clears statistics on the specified interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If no interface is specified, IPv4 URPF packet drop statistics on all interfaces are cleared by default.	
Configuration Examples	The following example clears IPv4 URPF packet drop statistics on port GigabitEthernet 0/1. <pre>FS# clear ip urpf interface gigabitEthernet0/1</pre> The following example clears IPv4 URPF packet drop statistics on all interfaces. <pre>FS# clear ip urpf</pre>	
Related Commands	Command	Description
	show ip urpf	Displays the URPF configuration and statistics.
Platform Description	N/A	

12.2 ip verify unicast source reachable-via (Interface Configuration Mode)

	Use this command to enable the IPv4 URPF feature in the interface configuration mode. Use the no form of this command to restore the default setting.	
	ip verify unicast source reachable-via { rx any } [allow-default]	
	no ip verify unicast	
Parameter Description	Parameter	Description
	rx	URPF check in the strict mode. In the strict mode, the egress port for the forwarding entry in the forwarding list found through the source address for the IP packet shall be matched with the ingress port.
	any	URPF check in the loose mode. In the loose mode, the forwarding entry for

		the source address for the IP packet can be found in the forwarding list.
	allow-default	(Optional) Allows using the default route to check URPF.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	To determine whether the route for the source address is in the forwarding list or not and the packet validity, enable the URPF feature to check the source address for the received IP packets. If no forwarding entry is matched, the packets are illegal. Enabling URPF feature in the interface configuration mode enables URPF check for the received packets on the interface. By default, the default route is not used for URPF check. Use the keyword <code>allow-default</code> to enable the URPF check. By default, the packets that failed to pass the URPF check are dropped. With ACL (<code>acl-name</code>) configured, the ACL matching continues when the routing fails. The packets will be dropped if the ACL is inexistent or the deny ACE is matched; otherwise, if the permit ACE is matched, the packets will be forwarded.  After this command is used, URPF check on IPv4 packets will be enabled.  This function is supported only on routed and Layer 3 interfaces, and have the following restrictions: ● Not support the ACL association; Not support to use the IPv6 route with prefix in 65 to 127 bits for the URPF check; ● After enabling the URPF feature, the range of packets received on the interface will be expanded, that is, the URPF feature is enabled for all packets received on the physical ports. ● After enabling the URPF feature, it halves the route forwarding capacity. ● After enabling the URPF feature in the strict mode, the user can match the equivalent route when URPF check is enabled for the packets received on the interface.  URPF feature cannot be configured in the global configuration mode and in the interface configuration mode at the same time.  URPF feature cannot be configured on range interface.	
Configuration Examples	The following example checks the URPF feature of the received packets in the strict mode on the interface GigabitEthernet 0/1. <pre>FS(config)# interface gigabitEthernet0/1 FS(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx</pre>	
Related Commands	Command	Description
	show ip urpf	Displays the URPF information.
Platform Description	N/A	

12.3 ip verify urpf drop-rate compute interval

	Use this command to set the URPF drop-rate compute interval. Use the no form of this command to restore the default setting.	
	ip verify urpf drop-rate compute interval <i>seconds</i>	
	no ip verify urpf drop-rate compute interval	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the URPF drop-rate compute interval, in the range from 30 to 300 in the unit of seconds.
Defaults	The default is 30 seconds.	
Command Mode	Global configuration mode	
Usage Guide	The URPF drop-rate is computed globally for both IPv4 and IPv6 packets on interfaces enabled with URPF.	
Configuration Examples	The following example sets the URPF drop-rate compute interval as 60 seconds. FS(config)# ip verify urpf drop-rate compute interval 60	
Related Commands	Command	Description
	ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
	ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
Platform Description	N/A	

12.4 ip verify urpf drop-rate notify

	Use this command to enable the URPF drop-rate monitoring. Use the no or default form of this command to restore the default setting.	
	ip verify urpf drop-rate notify	
	no ip verify urpf drop-rate notify	
	default ip verify urpf drop-rate notify	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	

Command Mode	Interface configuration mode	
Usage Guide	This command is used to enable the URPF drop-rate monitoring, notifying the user of the URPF packet drop information by means of Syslog or Trap for the convenience of the user network monitoring. URPF feature cannot be configured on range interface.	
Configuration Examples	The following example enables the URPF drop-rate monitoring on port GigabitEthernet 0/1. <pre>FS(config)# interface gigabitEthernet0/1 FS(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify</pre>	
Related Commands	Command	Description
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
Platform Description	N/A	

12.5 ip verify urpf drop-rate notify hold-down

	Use this command to set the URPF drop-rate notification interval. Use the no form of this command to restore to the default setting.	
	ip verify urpf drop-rate notify hold-down <i>seconds</i>	
	no ip verify urpf drop-rate notify hold-down	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the URPF drop-rate notification interval, in the range from 30 to 300 in the unit of seconds.
Defaults	The default is 300 seconds.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the URPF drop-rate notification interval as 60 seconds. <pre>FS(config)# ip verify urpf drop-rate notify hold-down 60</pre>	

Related Commands	Command	Description
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
	ip verify urpf drop-rate notify	Sets the URPF drop-rate monitoring.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
Platform Description	N/A	

12.6 ip verify urpf notification threshold

	Use this command to set the URPF drop-rate threshold. Use the no form of this command to restore the default setting.	
	ip verify urpf notification threshold <i>rate-value</i>	
	no ip verify urpf notification threshold	
Parameter Description	Parameter	Description
	threshold <i>rate-value</i>	Sets the URPF drop-rate threshold, in the range from 0 to 4,294,967,295 in the unit of packets per second (pps).
Defaults	The default is 1,000 pps.	
Command Mode	Interface configuration mode	
Usage Guide	The threshold 0 indicates that once the device detects a dropped packet due to the IPv4 URPF check, the notification is sent. The user can adjust the drop-rate threshold value according to the actual network performance. URPF feature cannot be configured on range interface.	
Configuration Examples	The following example sets the URPF drop-rate threshold 10pps on the interface GigabitEthernet 0/1. <pre>FS(config)# interface gigabitEthernet0/1 FS(config-if-GigabitEthernet 0/1)# ipv6 verify urpf drop-rate notify FS(config-if-GigabitEthernet 0/1)# ipv6 verify urpf notification threshold 10</pre>	
Related Commands	Command	Description
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate computing interval.
	ip verify urpf drop-rate notify	Sets the URPF drop-rate information monitoring.
	ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate notification interval.
Platform Description	N/A	

12.7 show ip urpf

	Use this command to display the IPv4 URPF configuration and statistics.													
	show ip urpf [interface <i>interface-name</i>]													
Parameter Description	Parameter	Description												
	interface <i>interface-name</i>	Displays the configuration and statistics on the specified interface.												
Defaults	N/A													
Command Mode	Privileged EXEC mode/Global configuration mode/Interface configuration mode													
Usage Guide	The global configuration and statistics of all interfaces are displayed by default.													
Configuration Examples	The following example displays IPv4 URPF configuration and statistics on port GigabitEthernet 0/1. <pre>FS# show ip urpf interface gigabitEthernet0/21 IP verify source reachable-via RX IP verify URPF drop-rate notify disabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 124 Number of drop-rate notification counts in this interface is 0</pre> <table><tr><th>Field</th><th>Description</th></tr><tr><td>IP verify source reachable-via xx</td><td>xx in strict mode is displayed as RX and in loose mode as ANY.</td></tr><tr><td>IP verify URPF drop-rate notify xx</td><td>If drop rate notification is enabled, xx is displayed as enabled. Otherwise, it is displayed as disabled.</td></tr><tr><td>IP verify URPF notification threshold is xxpps</td><td>The threshold of URPF drop rate, in the range from 0 to 4294967295 in the unit of packets per second (pps). The default is 1000.</td></tr><tr><td>Number of drop packets in this interface is x</td><td>The number of drop packets</td></tr><tr><td>Number of drop-rate notification counts in this interface is x</td><td>The URPF drop-rate notification counts</td></tr></table> The following example displays IPv4 URPF configuration and statistics. <pre>FS# show ip urpf IP verify URPF drop-rate compute interval is 30s IP verify URPF drop-rate notify hold-down is 300s Interface GigabitEthernet 0/1 IP verify source reachable-via RX IP verify URPF drop-rate notify disabled IP verify URPF notification threshold is 1000pps Number of drop packets in this interface is 124</pre>		Field	Description	IP verify source reachable-via xx	xx in strict mode is displayed as RX and in loose mode as ANY.	IP verify URPF drop-rate notify xx	If drop rate notification is enabled, xx is displayed as enabled. Otherwise, it is displayed as disabled.	IP verify URPF notification threshold is xxpps	The threshold of URPF drop rate, in the range from 0 to 4294967295 in the unit of packets per second (pps). The default is 1000.	Number of drop packets in this interface is x	The number of drop packets	Number of drop-rate notification counts in this interface is x	The URPF drop-rate notification counts
Field	Description													
IP verify source reachable-via xx	xx in strict mode is displayed as RX and in loose mode as ANY.													
IP verify URPF drop-rate notify xx	If drop rate notification is enabled, xx is displayed as enabled. Otherwise, it is displayed as disabled.													
IP verify URPF notification threshold is xxpps	The threshold of URPF drop rate, in the range from 0 to 4294967295 in the unit of packets per second (pps). The default is 1000.													
Number of drop packets in this interface is x	The number of drop packets													
Number of drop-rate notification counts in this interface is x	The URPF drop-rate notification counts													

	Number of drop-rate notification counts in this interface is 2	
	Field	Description
	IP verify URPF drop-rate compute interval is x	Drop-rate computing interval
	IP verify URPF drop-rate notify hold-down is x	Drop-rate notification interval
	Interface interface-name	interface-name is the name of the interface on which URPF is applied. Configuration and statistics on this interface are displayed.
Related Commands	Command	Description
	ip verify unicast source reachable-via	Enables the URPF features.
	ip verify urpf drop-rate compute interval	Sets the URPF drop-rate compute interval.
	ip verify urpf drop-rate notify hold-down	Sets the URPF drop-rate warning interval.
	ip verify urpf notification threshold	Sets the URPF drop-rate threshold.
	clear ip urpf	Clears the URPF statistical information.
Platform Description	N/A	

13 CPU Protection Commands

13.1 clear cpu-protect-counters

	Use this command to clear the CPP statistics.																																		
	clear cpu-protect counters [device <i>device_num</i>]																																		
Parameter Description	Parameter	Description																																	
	<i>device_num</i>	As a single physical device, there is no device parameter; As a stacking, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.																																	
Defaults	N/A																																		
Command Mode	Privileged EXEC mode																																		
Usage Guide	N/A																																		
Configuration Examples	The following example clears the CPP statistics. FS(config)#show cpu-protect type bpdu<table><tr><td>Packet Type</td><td>Traffic-class</td><td>Bandwidth(pps)</td><td>Rate(pps)</td><td>Drop(pps)</td><td>Total</td><td>Total Drop</td></tr><tr><td>bpdu</td><td>6</td><td>200</td><td>0</td><td>0</td><td>600</td><td>50</td></tr></table>FS#clear cpu-protect counters FS(config)#show cpu-protect type bpdu<table><tr><td>Packet Type</td><td>Traffic-class</td><td>Bandwidth(pps)</td><td>Rate(pps)</td><td>Drop(pps)</td><td>Total</td><td>Total Drop</td></tr><tr><td>bpdu</td><td>6</td><td>200</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table>							Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	bpdu	6	200	0	0	600	50	Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	bpdu	6	200	0	0	0	0
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop																													
bpdu	6	200	0	0	600	50																													
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop																													
bpdu	6	200	0	0	0	0																													
Related Commands	Command			Description																															
	N/A			N/A																															
Platform Description	N/A																																		

13.2 clear cpu-protect-counters mboard

	Use this command to clear the CPP statistics on the supervisor module.
	clear cpu-protect counters mboard

Parameter Description	Parameter	Description					
	N/A	N/A					
Defaults	N/A						
Command Mode	Privileged EXEC mode						
Usage Guide	N/A						
Configuration Examples	The following example clears the CPP statistics on the supervisor module.						
	FS(config)#show cpu-protect type bpdu						
	Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
	-----	-----	-----	-----	-----		
	bpdu	6	200	0	0	600	50
	FS#clear cpu-protect counters mboard						
	FS(config)#show cpu-protect type bpdu						
	Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
-----	-----	-----	-----	-----			
bpdu	6	200	0	0	0	0	
Related Commands	Command			Description			
	N/A			N/A			
Platform Description	N/A						

13.3 cpu-protect cpu bandwidth

	Use this command to configure the bandwidth for the CPU port. Use the no form of this command to restore the default setting.	
	cpu-protect cpu bandwidth <i>bandwidth_value</i>	
	no cpu-protect cpu bandwidth	
Parameter Description	Parameter	Description
	<i>bandwidth_value</i>	An integer number ranges from 0 to 100000 (PPS). Indicates the bandwidth value of the CPU port.
Defaults	The default CPU port bandwidth varies with products.	

Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the CPU port bandwidth to 32000pps. FS# configure terminal FS(config)# cpu-protect cpu bandwidth 32000 FS#show cpu-protect cpu %cpu port bandwidth: 32000(pps)	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

13.4 cpu-protect traffic-class bandwidth

	Use this command to configure the bandwidth for each priority queue. Use the no form of this command to restore the default setting.		
	cpu-protect traffic-class <i>traffic-class-num</i> bandwidth <i>bandwidth_value</i>		
	no cpu-protect traffic-class <i>traffic-class-num</i> bandwidth		
Parameter Description	Parameter	Description	
	<i>traffic-class-num</i>	A default integer that varies with products, indicating the queue priority	
	<i>bandwidth_value</i>	An integer number ranges from 0 to 100000 (pps). Indicates the bandwidth value of the CPU port.	
Defaults	The default bandwidth of each priority queue varies with products.		
Command Mode	Global configuration mode		
Usage Guide	N/A		
Configuration Examples	The following example s sets the priority queue 5 to 3500 pps. FS# configure terminal FS(config)# cpu-protect traffic-class 5 bandwidth 3500 FS#show cpu-protect traffic-class 5 Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) -----		

	5	3500	0	0
Related Commands	Command		Description	
	N/A		N/A	
Platform Description	N/A			

13.5 cpu-protect type bandwidth

	Use this command to configure the bandwidth of a specific packet. Use the no form of this command to restore the default setting.																				
	cpu-protect type <i>packet-type</i> bandwidth <i>bandwidth_value</i>																				
	no cpu-protect type <i>packet-type</i> bandwidth																				
Parameter Description	Parameter	Description																			
	<i>packet-type</i>	Packet type, which varies with products																			
	<i>bandwidth_value</i>	An integer number ranges from 0 to 32000 (pps). Indicates the bandwidth value of the CPU port.																			
Defaults	The default CPU port bandwidth varies with products.																				
Command Mode	Global configuration mode																				
Usage Guide	N/A																				
Configuration Examples	The following example sets the BPDU bandwidth to 200 pps. FS# configure terminal FS(config)# cpu-protect type bpdu bandwidth 200 FS(config)#show cpu-protect type bpdu <table><thead><tr><th>Packet Type</th><th>Traffic-class</th><th>Bandwidth(pps)</th><th>Rate(pps)</th><th>Drop(pps)</th><th>Total</th><th>Total Drop</th></tr></thead><tbody><tr><td>bpdu</td><td>6</td><td>200</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></tbody></table>							Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	bpdu	6	200	0	0	0	0
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop															
bpdu	6	200	0	0	0	0															
Related Commands	Command			Description																	
	N/A			N/A																	
Platform Description	N/A																				

13.6 cpu-protect type traffic-class

	Use this command to set the priority queue (PQ) of the packet. Use the no form of this command to restore the default setting.																				
	cpu-protect type <i>packet-type</i> traffic-class <i>traffic-class-num</i>																				
	no cpu-protect type <i>packet-type</i> traffic-class																				
Parameter Description	Parameter	Description																			
	<i>packet-type</i>	Packet type, which varies with products																			
	<i>traffic-class-num</i>	An integer number varying with products. Indicates the bandwidth value of the CPU port.																			
Defaults	The default PQ varies with products.																				
Command Mode	Global configuration mode																				
Usage Guide	N/A																				
Configuration Examples	The following example sets the PQ of BPDU packets to 5. FS# configure terminal FS(config)# cpu-protect type bpdu traffic-class 5 FS(config)#show cpu-protect type bpdu <table><thead><tr><th>Packet Type</th><th>Traffic-class</th><th>Bandwidth(pps)</th><th>Rate(pps)</th><th>Drop(pps)</th><th>Total</th><th>Total Drop</th></tr></thead><tbody><tr><td>bpdu</td><td>5</td><td>200</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></tbody></table>							Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	bpdu	5	200	0	0	0	0
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop															
bpdu	5	200	0	0	0	0															
Related Commands	Command			Description																	
	N/A			N/A																	
Platform Description	N/A																				

13.7 show cpu-protect

	Use this command to display all CPP configuration and statistics.	
	show cpu-protect [device <i>device_num</i>]	
Parameter Description	Parameter	Description
	<i>device_num</i>	As a single physical device, there is no device parameter; As a stacking, the device parameter indicates the chassis or the box-type device. If no device

		parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.
Defaults	N/A	
Command Mode	All configuraiton mode	
Usage Guide	N/A	
Configuration Examples	N/A	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

13.8 show cpu-protect cpu

	Use this command to display the configurations of the CPU port.	
	show cpu-protect cpu	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	All configuration modes	
Usage Guide	N/A	
Configuration Examples	The following example displays the configuration of the CPU port. <pre>FS#show cpu-protect cpu %cpu port bandwidth: 32000(pps)</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

13.9 show cpu-protect mboard

	Use this command to display the statistics of various packets of CPU protection on the management board.						
	show cpu-protect mboard						
Parameter Description	Parameter	Description					
	N/A	N/A					
Defaults	N/A						
Command Mode	All configuration modes						
Usage Guide	This command displays the statistics of the packets received by CPU on the management board.						
Configuration Examples	The following example displays the CPP configuration and statistics of the master device.						
	FS#show cpu-protect mboard						
	%cpu port bandwidth: 80000(pps)						
	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)			
	-----	-----	-----	-----			
	0	8000	0	0			
	1	8000	0	0			
	2	8000	0	0			
	3	8000	0	0			
	4	8000	0	0			
	5	8000	0	0			
	6	8000	0	0			
	7	8000	0	0			
	Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
	-----	-----	-----	-----	-----		
	bpdu	6	128	0	0	0	0
	arp	3	10000	0	0	0	0
	arp-dai	3	10000	0	0	0	0
	arp-proxy	3	10000	0	0	0	0
	tpp	7	128	0	0	0	0
	dot1x	4	128	0	0	0	0
	gvrp	5	128	0	0	0	0
	rldp	6	128	0	0	0	0
	lACP	6	128	0	0	0	0
	rerp	6	128	0	0	0	0

reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0
route-host-v4	0	4096	0	0	0	0
route-host-v6	0	4096	0	0	0	0
mld	0	1000	0	0	0	0
nd-snp-ns-na	6	128	0	0	0	0
nd-snp-rs	6	128	0	0	0	0
nd-snp-ra-redirect	6	128	0	0	0	0
nd-non-snp	6	128	0	0	0	0

	erps	4	128	0	0	0	0	
	mpls-ttl0	6	128	0	0	0	0	
	mpls-ttl1	6	128	0	0	0	0	
	mpls-ctrl	6	128	0	0	0	0	
	isis	5	2000	0	0	0	0	
	bgp	1	128	0	0	0	0	
	cfm	0	128	0	0	0	0	
	fcoe-fip	6	128	0	0	0	0	
	fcoe-local	6	128	0	0	0	0	
	bfd-echo	6	5120	0	0	0	0	
	bfd-ctrl	6	5120	0	0	0	0	
	madp	7	1000	0	0	0	0	
	ip4-other	6	128	0	0	0	0	
	ip6-other	6	128	0	0	0	0	
	non-ip-other	6	20000	0	0	0	0	
	trill	2	1000	0	0	0	0	
	trill-oam	2	1000	0	0	0	0	
	efm	2	1000	0	0	0	0	
	Related Commands	Command			Description			
	N/A			N/A				
Platform Description	N/A							

13.10 show cpu-protect summary

	Use this command to display the CPP configuration and statistics of the master device.	
	show cpu-protect summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	All configuration modes	
Usage Guide	N/A	
Configuration Examples	FS#show cpu-protect summary %cpu port bandwidth: 100000(pps)	

	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)			
0		6000	0	0			
1		6000	0	0			
2		6000	0	0			
3		6000	0	0			
4		6000	0	0			
5		6000	0	0			
6		6000	0	0			
7		6000	0	0			
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	
bpdu	6	128	0	0	0	0	
arp	1	3000	0	0	0	0	
tpp	6	128	0	0	0	0	
dot1x	2	1500	0	0	0	0	
gvrp	5	128	0	0	0	0	
rldp	5	128	0	0	0	0	
larp	5	256	0	0	0	0	
rrp	5	128	0	0	0	0	
reup	5	128	0	0	0	0	
lldp	5	768	0	0	0	0	
cdp	5	768	0	0	0	0	
dhcps	2	1500	0	0	0	0	
dhcps6	2	1500	0	0	0	0	
dhcp6-client	2	1500	0	0	0	0	
dhcp6-server	2	1500	0	0	0	0	
dhcp-relay-c	2	1500	0	0	0	0	
dhcp-relay-s	2	1500	0	0	0	0	
option82	2	1500	0	0	0	0	
tunnel-bpdu	2	128	0	0	0	0	
tunnel-gvrp	2	128	0	0	0	0	
unknown-v6mc	1	128	0	0	0	0	
xgv6-ipmc	1	128	0	0	0	0	
stargv6-ipmc	1	128	0	0	0	0	
unknown-v4mc	1	128	0	0	0	0	
xgv-ipmc	2	128	0	0	0	0	
stargv-ipmc	2	128	0	0	0	0	
udp-helper	1	128	0	0	0	0	
dvmrp	4	128	0	0	0	0	
igmp	2	1000	0	0	0	0	
icmp	3	1600	0	0	0	0	
ospf	4	2000	0	0	0	0	
ospf3	4	2000	0	0	0	0	

pim	4	1000	0	0	0	0
pimv6	4	1000	0	0	0	0
rip	4	128	0	0	0	0
ripng	4	128	0	0	0	0
vrrp	6	256	0	0	0	0
vrrpv6	6	256	0	0	0	0
ttl0	0	128	0	0	0	0
ttl1	0	2000	0	0	0	0
hop-limit	0	800	0	0	0	0
local-ipv4	3	4000	0	0	0	0
local-ipv6	3	4000	0	0	0	0
v4uc-route	1	800	0	0	0	0
v6uc-route	1	800	0	0	0	0
rt-host	4	3000	0	0	0	0
mld	2	1000	0	0	0	0
nd-snp-ns-na	1	3000	0	0	0	0
nd-snp-rs	1	1000	0	0	0	0
nd-snp-ra-redirect	1	1000	0	0	0	0
erps	5	128	0	0	0	0
mpls-ttl0	4	128	0	0	0	0
mpls-ttl1	4	128	0	0	0	0
mpls-ctrl	4	128	0	0	0	0
isis	4	2000	0	0	0	0
bgp	4	2000	0	0	0	0
cfm	5	512	0	0	0	0
web-auth	2	2000	0	0	0	0
fcoe-fip	4	1000	0	0	0	0
fcoe-local	4	1000	0	0	0	0
bfd	6	5120	0	0	0	0
micro-bfd	6	5120	0	0	0	0
micro-bfd-v6	6	5120	0	0	0	0
dldp	6	3200	0	0	0	0
other	0	4096	0	0	0	0
trill	4	1000	0	0	0	0
efm	5	1000	0	0	0	0
ipv6-all	0	2000	0	0	0	0
ip-option	0	800	0	0	0	0
mgmt	-	4000	4	0	4639	0
dns	2	200	0	0	0	0
sdn	0	5000	0	0	0	0
sdn_of_fetch	0	5000	0	0	0	0
sdn_of_copy	0	5000	0	0	0	0
sdn_of_trap	0	5000	0	0	0	0
vxlan-non-uc	1	512	0	0	0	0

	local-telnet	3	1000	0	0	0	0
	local-snmp	3	1000	0	0	0	0
	local-ssh	3	1000	0	0	0	0
Related Commands	Command			Description			
	N/A			N/A			
Platform Description	N/A						

13.11 show cpu-protect traffic-class

	Use this command to display the summarized configuration and statistics of priority queues.			
	show cpu-protect traffic-class { <i>traffic-class-num</i> all } [device <i>device_num</i>]			
Parameter Description	Parameter	Description		
	<i>traffic-class-num</i>	A default integer that varies with products, indicating the queue priority.		
	<i>all</i>	Displays configurations and statistics of all priority queues.		
	<i>device_num</i>	As a single physical device, there is no device parameter; As a stacking, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.		
Defaults	N/A			
Command Mode	All configuration modes			
Usage Guide	N/A			
Configuration Examples	The following example displays the summarized configuration and statistics of priority queues.			
	FS#show cpu-protect traffic-class all			
	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)
	-----	-----	-----	
	0	8000	0	0
	1	8000	0	0
	2	8000	0	0
	3	8000	0	0
	4	8000	0	0
	5	3200	0	0
	6	8000	0	0
	7	8000	0	0

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

13.12 show cpu-protect type

	Use this command to display the statistics of the specified type of packets																				
	show cpu-protect type <i>packet-type</i> [device <i>device_num</i>]																				
Parameter Description	Parameter	Description																			
	<i>packt-type</i>	Packet type, which varies with products																			
	<i>all</i>	Displays the configurations and statistics of all packet types.																			
	<i>device_num</i>	As a single physical device, there is no device parameter; As a stacking, the device parameter indicates the chassis or the box-type device. If no device parameter is specified, that indicates this command takes effect to the master chassis or the master box-type device.																			
Defaults	N/A																				
Command Mode	All configuration modes																				
Usage Guide	N/A																				
Configuration Examples	The following example displays the statistics of the ICMP packets. FS(config)#show cpu-protect type icmp<table><tr><th>Packet Type</th><th>Traffic-class</th><th>Bandwidth(pps)</th><th>Rate(pps)</th><th>Drop(pps)</th><th>Total</th><th>Total Drop</th></tr><tr><td>icmp</td><td>5</td><td>1500</td><td>50</td><td>0</td><td>10000</td><td>100</td></tr></table>							Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop	icmp	5	1500	50	0	10000	100
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop															
icmp	5	1500	50	0	10000	100															
Related Commands	Command			Description																	
	N/A			N/A																	
Platform Description	N/A																				

14 DHCP Snooping Commands

14.1 clear ip dhcp snooping binding

	Use this command to delete the dynamic user information from the DHCP Snooping binding database.	
	clear ip dhcp snooping binding [<i>ip</i>] [<i>mac</i>] [vlan <i>vlan-id</i>] [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the user MAC address to be cleared.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ip</i>	Specifies the IP address to be cleared.
	<i>interface-id</i>	Specifies the ID of the interface to be cleared.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command to clear the current dynamic user information from the DHCP Snooping binding database.  After this command is used, all the DHCP clients connecting interfaces with IP Source Guard function enabled should request IP addresses again, or they cannot access network.	
Configuration Examples	The following example clears the dynamic database information from the DHCP Snooping binding database. <pre>FS# clear ip dhcp snooping binding FS# show ip dhcp snooping binding Total number of bindings: 0 MacAddress IpAddress Lease(sec) Type VLAN Interface -----</pre>	
Related Commands	Command	Description
	show ip dhcp snooping binding	Displays the information of the DHCP Snooping binding database.
Platform Description	N/A	

14.2 ip dhcp snooping

	Use this command to enable the DHCP Snooping function globally.
	Use the no form of this command to restore the default setting.

	ip dhcp snooping	
	no ip dhcp snooping	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The show ip dhcp snooping command is used to display whether the DHCP Snooping function is enabled.	
Configuration Examples	The following example enables the DHCP Snooping function. <pre>FS# configure terminal FS(config)# ip dhcp snooping FS(config)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the configuration information of DHCP Snooping.
	ip dhcp snooping vlan	Configures DHCP Snooping enabled VLAN.
Platform Description	N/A	

14.3 ip dhcp snooping bootp-bind

	Use this command to enable DHCP Snooping BOOTP-bind function. Use the no form of this command to restore the default setting.	
	ip dhcp snooping bootp-bind	
	no ip dhcp snooping bootp-bind	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	

Usage Guide	By default, the DHCP Snooping only forwards BOOTP packets. With this function enabled, it can Snoop BOOTP packets. After the BOOTP client requests an address successfully, the DHCP Snooping adds the BOOTP user to the static binding database.	
Configuration Examples	The following example enables the DHCP Snooping BOOTP-bind function. <pre>FS# configure terminal FS(config)# ip dhcp snooping bootp-bind FS(config)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.
Platform Description	N/A	

14.4 ip dhcp snooping check-giaddr

	Use this command to enable DHCP Snooping to support the function of processing Relay requests. Use the no form of this command to restore the default setting.	
	ip dhcp snooping check-giaddr	
	no ip dhcp snooping check-giaddr	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After the feature is enabled, services using DHCP Snooping binding entries generated based on Relay requests, such as IP Source Guard/802.1x authentication, cannot be deployed. Otherwise, users fail to access the Internet. After the feature is enabled, the ip dhcp snooping verify mac-address command cannot be used. Otherwise, DHCP Relay requests will be discarded and as a result, users fail to obtain addresses.	
Configuration Examples	The following example enables DHCP Snooping to support the function of processing Relay requests. <pre>FS# configure terminal FS(config)# ip dhcp snooping check-giaddr FS(config)# end</pre>	

Related Commands	Command	Description
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
Platform Description	N/A	

14.5 ip dhcp snooping database

	Use this command to configure file backup of the DHCP Snooping binding database. Use the no form of this command to restore the default setting.	
	ip dhcp snooping database sata0 [interval <i>time</i>]	
	no ip dhcp snooping database sata0	
Parameter Description	Parameter	Description
	<i>time</i>	Indicates the interval of storing the database in the unit of second. The range is from 10s to 86,400s. The default value is 300s.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After this feature is enabled, the DHCP Snooping database can be written to the backup file of a specified type. In this way, users are able to resume communication immediately after restart of the device.	
Configuration Examples	The following example sets configures file backup of the DHCP Snooping binding database with the default interval. <pre>FS# configure terminal FS(config)# ip dhcp snooping database sata0 FS(config)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
	show run	Displays the current backup mode.
Platform Description	N/A	

14.6 ip dhcp snooping database write-delay

	Use this command to configure the switch to write the dynamic user information of the DHCP Snooping binding database into the flash periodically. Use the no form of this command to restore the default setting.	
	ip dhcp snooping database write-delay <i>time</i>	
	no ip dhcp snooping database write-delay	
Parameter Description	Parameter	Description
	<i>time</i>	The interval at which the system writes the dynamic user information of the DHCP Snooping database into the flash, in the range from 600 to 86,400 in the unit of seconds
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This function writes user information into flash in case of loss after restart. In that case, users need to obtain IP addresses again for normal communication.  Too fast writing will reduce flash durability.	
Configuration Examples	The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds. <pre>FS# configure terminal FS(config)# ip dhcp snooping database write-delay 3600 FS(config)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the configuration information of the DHCP Snooping.
Platform Description	N/A	

14.7 ip dhcp snooping database write-to-flash

	Use this command to write the dynamic user information of the DHCP binding database into flash in real time.
	ip dhcp snooping database write-to-flash

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	This command is used to write the dynamic user information of the DHCP binding database into flash in real time.	
Configuration Examples	The following example writes the dynamic user information of the DHCP binding database into flash. <pre>FS# configure terminal FS(config)# ip dhcp snooping database write-to-flash FS(config)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

14.8 ip dhcp snooping information option

	Use this command to add option82 to the DHCP request message. Use the no form of this command to restore the default setting.	
	ip dhcp snooping information option [standard-format]	
	no ip dhcp snooping information option [standard-format]	
Parameter Description	Parameter	Description
	standard-format	The option82 uses the standard format.
Defaults	This function is disabled by default,	
Command Mode	Global configuration mode	
Usage Guide	This command adds option82 to the DHCP request messages based on which the DHCP server assigns IP addresses. By default, this function is in extended mode.  DHCP Relay function adds option82 by default. Therefore, it is unnecessary to enable functions of DHCP	

	Snooping option82 and DHCP Relay at the same time.	
Configuration Examples	The following example adds option82 to the DHCP request message. <pre>FS# configure terminal FS(config)# ip dhcp snooping information option FS(config)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.
Platform Description	N/A	

14.9 ip dhcp snooping information option format remote-id

	Use this command to set the option82 sub-option remote-id as the customized character string. Use the no form of this command to restore the default setting.	
	ip dhcp snooping information option format remote-id { string <i>ascii-string</i> hostname }	
	no ip dhcp snooping information option format remote-id { string <i>ascii-string</i> hostname }	
Parameter Description	Parameter	Description
	string <i>ascii-string</i>	The content of the option82 remote-id extension format is customized character string.
	hostname	The content of the option82 remote-id extension format hostname
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This command sets the remote-id in the option82 to be added to the DHCP request message as the customized character string. The DHCP server will assign the IP address according to the option82 information.	
Configuration Examples	The following example adds the option82 into the DHCP request packets with the content of remote-id as hostname. <pre>FS# configure terminal FS(config)# ip dhcp snooping information option format remote-id hostname</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

14.10 ip dhcp snooping monitor

	Use this command to enable DHCP Snooping monitoring. Use the no form of this command to restore the default setting.	
	ip dhcp snooping monitor	
	no ip dhcp snooping monitor	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	After the feature is enabled, DHCP Snooping generates binding entries according to the interaction process by copying DHCP packets. It, however, does not check the validity of packets.	
Configuration Examples	The following example enables DHCP Snooping monitoring. <pre> FS# configure terminal FS(config)# ip dhcp snooping monitor FS(config)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

14.11 ip dhcp snooping suppression

	Use this command to set the port to be the suppression status. Use the no form of this command to restore the default setting.	
	ip dhcp snooping suppression	
	no ip dhcp snooping suppression	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode/WLAN security configuration mode	
Usage Guide	This command denies all DHCP request messages under the port, that is, all the users under the port are prohibited to request IP addresses through DHCP. This command is only supported on Layer 2 switch interfaces and aggregate ports (APs).	
Configuration Examples	The following example sets fastEthernet 0/2 and WLAN 1 to be in the suppression status. <pre> FS# configure terminal FS(config)# interface fastEthernet 0/2 FS(config-if)# ip dhcp snooping suppression FS(config-if)# end FS# configure terminal FS(config)# wlansec 1 FS(config-wlansec)# ip dhcp snooping suppression FS(config-if-wlansec)# end </pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.
Platform Description	N/A	

14.12 ip dhcp snooping trust

	Use this command to set the trusted ports for DHCP Snooping. Use the no form of this command to restore the default setting.	
	ip dhcp snooping trust	
	no ip dhcp snooping trust	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	All ports are untrusted by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to set a port as a trusted port. The DHCP response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. This	

	command is only supported on Layer 2 switch interfaces and aggregate ports (APs).	
Configuration Examples	The following example sets fastEthernet 0/1 as a trusted port: <pre>FS# configure terminal FS(config)# interface fastEthernet 0/1 FS(config-if)# ip dhcp snooping trust FS(config-if)# end</pre>	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.
Platform Description	N/A	

14.13 ip dhcp snooping verify mac-address

	Use this command to check whether the source MAC address of the DHCP request message matches against the client addr field of the DHCP message. Use the no form of this command to restore the default setting.	
	ip dhcp snooping verify mac-address	
	no ip dhcp snooping verify mac-address	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to check the source MAC address of the DHCP request message. If the MAC address in the link-layer header is different from the CHADDR (Client MAC Address), the check fails ,and the packets will be discarded.	
Configuration Examples	The following example enables the check of the source MAC address of the DHCP request message. FS# configure terminal FS(config)# ip dhcp snooping verify mac-address FS(config)# end	
Related Commands	Command	Description
	show ip dhcp snooping	Displays the DHCP Snooping configuration.

Platform	N/A
Description	

14.14 ip dhcp snooping vlan

	Use this command to enable DHCP Snooping for the specific VLAN. Use the no form of this command to restore the default setting.	
	ip dhcp snooping vlan {vlan-rng { vlan-min [vlan-max] }}	
	no ip dhcp snooping vlan {vlan-rng { vlan-min [vlan-max] }}	
Parameter Description	Parameter	Description
	<i>vlan-rng</i>	VLAN range of effective DHCP Snooping
	<i>vlan-min</i>	Minimum VLAN of effective DHCP Snooping
	<i>vlan-max</i>	Maximum VLAN of effective DHCP Snooping
Defaults	By default, once the DHCP Snooping is enabled globally, it takes effect for all VLANs.	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enable DHCP Snooping for specified VLANs globally.	
Configuration Examples	The following example enables the DHCP Snooping function in VLAN 1000. <pre>FS# configure terminal FS(config)# ip dhcp snooping vlan 1000 FS(config)# end</pre> The following example enables the DHCP Snooping function from VLAN1 to VLAN10. <pre>FS# configure terminal FS(config)# ip dhcp snooping vlan 1-10 FS(config)# end</pre>	
Related Commands	Command	Description
	ip dhcp snooping	Enables DHCP Snooping globally.
Platform	N/A	
Description		

14.15 renew ip dhcp snooping database

	Use this command to import the information in current flash to the DHCP Snooping binding database manually as needed.

	renew ip dhcp snooping database	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to import the flash file information to the DHCP Snooping database in real time.  Records out of lease time and repeated will be neglected.	
Configuration Examples	The following example imports the flash file information to the DHCP Snooping database. <pre>FS# renew ip dhcp snooping database</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

14.16 show ip dhcp snooping

	Use this command to display the DHCP Snooping configuration.	
	show ip dhcp snooping	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the DHCP Snooping configuration. <pre>FS# show ip dhcp snooping</pre> Switch DHCP snooping status :ENABLE	

Verification of hwaddr field status :DISABLE DHCP snooping database write-delay time: 0 seconds DHCP snooping option 82 status: ENABLE DHCP snooping Support Bootp bind status: ENABLE <table> <tr> <th>Interface</th><th>Trusted</th><th>Rate limit(pps)</th></tr> <tr> <td>GigabitEthernet 0/4</td><td>YES</td><td>unlimited</td></tr> <tr> <td>Default</td><td>No</td><td></td></tr> </table>			Interface	Trusted	Rate limit(pps)	GigabitEthernet 0/4	YES	unlimited	Default	No	
Interface	Trusted	Rate limit(pps)									
GigabitEthernet 0/4	YES	unlimited									
Default	No										
Related Commands	Command	Description									
	ip dhcp snooping	Enables the DHCP Snooping globally.									
	ip dhcp snooping verify mac-address	Enables the check of source MAC address of DHCP Snooping packets.									
	ip dhcp snooping write-delay	Sets the interval of writing user information to FLASH periodically.									
	ip dhcp snooping information option	Adds option82 to the DHCP request message.									
	ip dhcp snooping bootp-bind	Enables the DHCP Snooping bootp bind function.									
	ip dhcp snooping trust	Sets the port as a trust port.									
Platform Description	N/A										

14.17 show ip dhcp snooping binding

	Use this command to display the information of the DHCP Snooping binding database.						
	show ip dhcp snooping binding						
Parameter Description	Parameter		Description				
	N/A		N/A				
Defaults	N/A						
Command Mode	Privileged EXEC mode						
Usage Guide	This command is used to display all the information of the DHCP Snooping binding database.						
Configuration Examples	1: The following example displays the information of the DHCP Snooping binding database.						
	FS# show ip dhcp snooping binding						
	Total number of bindings: 1						
	NO.	MACADDRESS	IPADDRESS	LEASE(SEC)	TYPE	VLAN	INTERFACE

	1	0000.0000.0001	1.1.1.1	78128	DHCP-Snooping 1	GigabitEthernet 0/1	
	2	0000.0000.0002	2.2.2.2	78111	DHCP-Snooping 1	WLAN 1	
	2: For products supporting QINQ termination, the following example displays the information of the inner VLAN.						
	FS# show ip dhcp snooping binding						
	Total number of bindings: 1						
	NO.	MACADDRESS	IPADDRESS	LEASE(SEC)	TYPE	VLAN	INNER-VLAN
	INTERFACE						

	1	0000.0000.0001	1.1.1.1	78128	DHCP-Snooping	1	10
	GigabitEthernet 0/1						
	3: For products supporting VXLAN, the following example displays the information of the VXLAN.						
	FS# show ip dhcp snooping binding						
Total number of bindings: 1							
NO.	MACADDRESS	IPADDRESS	LEASE(SEC)	TYPE	VLAN	INNER-VLAN	VXLAN
INTERFACE							

1	0000.0000.0001	1.1.1.1	78128	DHCP-Snooping	0	0	1
GigabitEthernet 0/1							
Related Commands	Command			Description			
	ip dhcp snooping binding			Adds the static user information to the DHCP Snooping database.			
	clear ip dhcp snooping binding			Clears the dynamic user information from the DHCP Snooping binding database.			
Platform Description	N/A						

15 DHCPv6 Snooping Commands

15.1 clear ipv6 dhcp snooping binding

	Use this command to clear all the user information in the DHCPv6 Snooping binding database.	
	clear ipv6 dhcp snooping binding [<i>mac</i> vlan <i>vlan-id</i> <i>ipv6-address</i> interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the MAC address to be deleted.
	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.
	<i>ipv6-address</i>	Specifies the IPv6 address to be cleared.
	<i>interface-id</i>	Specifies the interface to be cleared.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the generated user information in the DHCPv6 Snooping binding database.	
Configuration Examples	The following example clears all the user information in the DHCPv6 Snooping binding database. <pre> FS# clear ipv6 dhcp snooping binding FS# show ipv6 dhcp snooping binding NO. MacAddress IPv6 Address Lease(sec) VLAN Interface FilterType FilterStatus ----- Total number of bindings: 0 </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.2 clear ipv6 dhcp snooping prefix

	Use this command to clear all the user information in the DHCPv6 Snooping prefix list.	
	clear ipv6 dhcp snooping prefix [<i>mac</i> vlan <i>vlan-id</i> <i>ipv6-prefix</i> interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>mac</i>	Specifies the MAC address to be deleted.

	<i>vlan-id</i>	Specifies the ID of the VLAN to be cleared.						
	<i>ipv6-address</i>	Specifies the IPv6 address to be cleared.						
	<i>interface-id</i>	Specifies the interface to be cleared.						
Defaults	N/A							
Command Mode	Privileged EXEC mode							
Usage Guide	This command is used to clear the generated user information in the DHCPv6 Snooping prefix list.							
Configuration Examples	The following example clears all the user information in the DHCPv6 Snooping binding database							
	FS# clear ipv6 dhcp snooping prefix							
	FS# show ipv6 dhcp snooping prefix							
	NO.	MacAddress	IPv6 Prefix	Lease(sec)	VLAN	Interface	FilterType	FilterStatus
	---	-----	-----	---	-----	-----	-----	-----
	Total number of prefixes: 0							
Related Commands	Command					Description		
	N/A					N/A		
Platform Description	N/A							

15.3 clear ipv6 dhcp snooping statistics

	Use this command to clear the statistical information of the DHCPv6 packets.	
	clear ipv6 dhcp snooping statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to clear the statistical information of the DHCPv6 packets.	
Configuration Examples	The following example clears the statistical information of the DHCPv6 packets. <pre>FS# clear ipv6 dhcp snooping statistics FS# show ipv6 dhcp snooping statistics</pre>	

	Packets Processed by DHCPv6 Snooping = 0 Packets Dropped Because Received on untrusted ports = 0 Relay forward = 0 No binding entry = 0 Binding fail = 0 Unknown packet = 0 Unknown output interface = 0 No enough memory = 0 Admin filter-dhcpv6-pkt = 0	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.4 ipv6 dhcp snooping

	Use this command to enable the DHCPv6 Snooping function globally. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping	
	no ipv6 dhcp snooping	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	The show ip dhcpv6 snooping command is used to display whether the DHCPv6 Snooping function is enabled.	
Configuration Examples	The following example enables the DHCPv6 Snooping function globally. FS# configure terminal FS(config)# ipv6 dhcp snooping FS(config)# end	
Related Commands	Command	Description
	show ipv6 dhcp snooping	Displays the DHCPv6 Snooping .

Platform	N/A
Description	

15.5 ipv6 dhcp snooping binding-delay

	Use this command to add the dynamic binding entry to the hardware filtering list after the delay. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping binding-delay <i>seconds</i>	
	no ipv6 dhcp snooping binding-delay	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the binding delay time.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	By default, the dynamic binding entries are added to the hardware filtering list in real time. With this command configured, if no IPv6 address conflict is detected within the specified time, the dynamic binding entries are added to the hardware filtering list.	
Configuration Examples	The following example sets the delay to 10 seconds. FS(config)# ipv6 dhcp snooping binding-delay 10	
Related Commands	Command	Description
	N/A	N/A
Platform	N/A	
Description		

15.6 ipv6 dhcp snooping database write-delay

	Use this command to write the dynamic user information of the DHCPv6 Snooping binding database into the flash periodically. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping database write-delay <i>time</i>	
	no ipv6 dhcp snooping database write-delay	
Parameter Description	Parameter	Description
	<i>time</i>	The interval ranging from 600 to 86,400 in the unit of seconds, at which the

		system writes the dynamic user information of the DHCP Snooping database into the flash.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	This function writes user information into flash and can avoid loss after restart. In that case, users need to obtain IP addresses again for normal communication.  Too fast writing will reduce flash durability.	
Configuration Examples	The following example sets the interval at which the switch writes the user information into the flash to 3,600 seconds. <pre>FS# configure terminal FS(config)# ip dhcp snooping database write-delay 3600 FS(config)# end</pre>	
Related Commands	Command	Description
	show ipv6 dhcp snooping	Displays the DHCPv6 Snooping configuration.
Platform Description	N/A	

15.7 ipv6 dhcp snooping database write-to-flash

	Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.	
	ipv6 dhcp snooping database write-to-flash	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Use this command to write the dynamic user information of the DHCPv6 binding database into flash in real time.	
Configuration Examples	The following example writes the dynamic user information of the DHCPv6 binding database into flash. <pre>FS# configure terminal</pre>	

	FS(config)# ipv6 dhcp snooping database write-to-flash FS(config)# end	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.8 ipv6 dhcp snooping information option

	Use this command to add option18/37 to the DHCPv6 request packets. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping information option [standard-format]	
	no ipv6 dhcp snooping information option [standard-format]	
Parameter Description	Parameter	Description
	standard-format	The Option18/37 uses the standard format.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured, the option18/37 will be added to the DHCPv6 request packets and the DHCPv6 server will assign the addresses according to the option18/37 information. Use this command without parameter standard-format to enable the standard format.	
	 DHCPv6 Relay function adds option18/37 by default. Therefore, it is unnecessary to enable functions of DHCP Snooping option18/37 and DHCPv6 Relay at the same time.	
Configuration Examples	The following example adds the option18/37 into the DHCPv6 packets.	
	<pre> FS# configure terminal FS(config)# ipv6 dhcp snooping information option FS(config)# end FS# show ipv6 dhcp snooping Switch DHCPv6 snooping status :ENABLE DHCPv6 snooping vlan: 1-4094 DHCPv6 snooping database write-delay time: 0 seconds DHCPv6 snooping option 18/37 status: ENABLE DHCPv6 snooping link detection :DISABLE Interface Trusted Filter DHCP </pre>	

	FastEthernet0/10	yes	DISABLE
Related Commands	Command	Description	
	show ipv6 dhcp snooping	Displays the configuration information of the DHCPv6 Snooping.	
Platform Description	N/A		

15.9 ipv6 dhcp snooping information option format remote-id

	Use this command to add option37 remote-id customized character string into the DHCPv6 request packets. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping information option format remote-id [string <i>ascii-string</i> hostname]	
	no ipv6 dhcp snooping information option format remote-id [string <i>ascii-string</i> hostname]	
Parameter Description	Parameter	Description
	string <i>ascii-string</i>	The content of Option37 remote-id extension format is customized character string.
	hostname	The content of Option37 remote-id extension format is hostname.
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	With this command configured, the option37 remote-id will be added to the DHCPv6 request packets with the content as the customized and the DHCPv6 server will assign the addresses according to the option37 information.	
Configuration Examples	The following example adds the option37 remote-id to the DHCPv6 request packets with the content being hostname. <pre>FS# configure terminal FS(config)# ipv6 dhcp snooping information option format remote-id hostname</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.10 ipv6 dhcp snooping filter-dhcp-pkt

	Use this command to filter all received DHCPv6 request packets. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping filter-dhcp-pkt	
	no ipv6 dhcp snooping filter-dhcp-pkt	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to filter all received DHCPv6 request packets, that is, to avoid all the DHCPv6 users on this interface to apply for the addresses. This command is valid only on 2-layer wired switch ports, aggregate ports and sub interfaces as well as in air interfaces.	
Configuration Examples	The following example filters all DHCPv6 request packets on interface FastEthernet 0/1 and WLAN 1. <pre> FS# configure terminal FS(config)# interface GigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)# ipv6 dhcp snooping filter-dhcp-pkt FS(config-if-GigabitEthernet 0/2)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.11 ipv6 dhcp snooping link-detection

	Use this command to clear the dynamic binding entry on an interface when the interface links down. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping link-detection	
	no ipv6 dhcp snooping link-detection	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	This function is disabled by default.				
Command Mode	Global configuration mode				
Usage Guide	By default, the dynamic binding entries are not cleared on a wired interface when the interface links down. With this function enabled, the dynamic binding entries are auto-cleared on an interface when the interface is in the LINK DOWN status.				
Configuration Examples	The following example clears the dynamic binding entry on a wired interface when the interface is in the LINK DOWN status. <pre>FS# configure terminal FS(config)# ipv6 dhcp snooping link-detection</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show ipv6 dhcp snooping</td><td>Displays the configuration information of the DHCPv6 Snooping.</td></tr> </table>	Command	Description	show ipv6 dhcp snooping	Displays the configuration information of the DHCPv6 Snooping.
Command	Description				
show ipv6 dhcp snooping	Displays the configuration information of the DHCPv6 Snooping.				
Platform Description	N/A				

15.12 ipv6 dhcp snooping trust

	Use this command to set the specified DHCPv6 Snooping ports as the trusted ports. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping trust	
	no ipv6 dhcp snooping trust	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	All ports are untrusted ports by default.	
Command Mode	Interface configuration mode	
Usage Guide	1. Use this command to set a port as a trusted port. The DHCPv6 Server response messages received under the trust port are forwarded normally, but the response messages received under the untrusted port will be discarded. 2. This command is valid only on Layer 2 wired switch ports and aggregate ports.	

Configuration Examples	The following example sets FastEthernet 0/1 as a trust port:	
	<pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if)# ipv6 dhcp snooping trust FS(config-if)# end</pre>	
Related Commands	Command	Description
	show ipv6 dhcp snooping	Displays the DHCPv6 Snooping configuration.
Platform Description	N/A	

15.13 ipv6 dhcp snooping vlan

	Use this command to enable DHCPv6 Snooping for the specific VLAN. Use the no form of this command to disable this function.	
	ipv6 dhcp snooping vlan { <i>vlan-rng</i> { <i>vlan-min</i> [<i>vlan-max</i>] } }	
	no ipv6 dhcp snooping vlan { <i>vlan-rn</i> { <i>vlan-min</i> [<i>vlan-max</i>] } }	
Parameter Description	Parameter	Description
	<i>vlan-rng</i>	Sets the valid VLAN range.
	<i>vlan-min</i>	Minimum VLAN ID
	<i>vlan-max</i>	Maximum VLAN ID
Defaults	By default, once the DHCPv6 Snooping is enabled globally, it takes effect for all VLANs.	
Command Mode	Global configuration mode	
Usage Guide	With the global DHCPv6 snooping enabled, this function is enabled in all VLANs by default.	
Configuration Examples	The following example enables the DHCPv6 Snooping function in VLAN 1000. <pre>FS# configure terminal FS(config)# ipv6 dhcp snooping vlan 1000 FS(config)# end</pre>	
	The following example enables the DHCPv6 Snooping function in VLAN 1 to VLAN 10. <pre>FS# configure terminal FS(config)# ipv6 dhcp snooping vlan 1-10 FS(config)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.14 ipv6 dhcp snooping vlan information option change-vlan-to vlan

	Use this command to enable the function of adding the option18 interface-is into the DHCP request packets and change the VLAN to the specified VLAN for the forwarding. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping vlan <i>vlan-id</i> information option change-vlan-to vlan <i>vlan-id</i>	
	no ipv6 dhcp snooping vlan <i>vlan-id</i> information option change-vlan-to vlan <i>vlan-id</i>	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	Specifies the ID of the VLAN to be replaced.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	With this command enabled, the option18 interface-id will be added into the DHCPv6 request packets and the VLAN will be changed to the specified one and the DHCP server will assign the addresses according to the optionq8 information.	
Configuration Examples	The following example adds the option18 interface-id into the DHCPv6 request packets and changes the VLAN4094 in the option to VLAN 4093. <pre> FS# configure terminal FS(config)# interface fastEthernet 0/1 FS(config-if)# ipv6 dhcp snooping vlan 4094 information option change-vlan-to vlan 4093 FS(config-if)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.15 ipv6 dhcp snooping vlan information option format-type interface-id string

	Use this command to enable the function of adding the option18 into the DHCP request packets and filling the option18 interface-id with the content being the user-defined (the storage format is ASCII) and performing the packet forwarding. Use the no form of this command to restore the default setting.	
	ipv6 dhcp snooping vlan <i>vlan-id</i> information option format-type interface-id string <i>ascii-string</i>	
	no ipv6 dhcp snooping vlan <i>vlan-id</i> information option format-type interface-id string <i>ascii-string</i>	

Parameter Description	Parameter	Description
	<i>vlan-id</i>	The VLAN where the DHCPv6 request packets are
	<i>ascii-string</i>	User-defined content for filling the interface-id
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	With this command configured, the option18 interface-id will be added into the DHCPv6 request packets with the content being user-defined and the DHCPv6 server will assign the addresses according to the option18 information.	
Configuration Examples	The following example adds the option18 interface-id to the DHCPv6 request packets with the content being <i>port-name</i>. <pre> FS# configure terminal FS(config)# interface fastEthernet 0/1 FS(config-if)# ipv6 dhcp snooping vlan 4094 information option format-type interface-id string port-name FS(config-if)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.16 renew ipv6 dhcp snooping database

	Use this command to import the information in current flash to the DHCPv6 Snooping binding database manually as needed.	
	renew ipv6 dhcp snooping database	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to import the flash file information to the DHCPv6 Snooping database in real time.	

	 Records out of lease time and repeated will be neglected.	
Configuration Examples	The following example imports the flash file information to the DHCPv6 Snooping database. <pre>FS# renew ipv6 dhcp snooping database</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.17 show ipv6 dhcp snooping

	Use this command to display the setting of the DHCPv6 Snooping.	
	show ipv6 dhcp snooping	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the setting of the DHCPv6 Snooping. <pre>FS# show ipv6 dhcp snooping Switch DHCPv6 snooping status :ENABLE DHCPv6 snooping vlan: 1-4094 DHCPv6 snooping database write-delay time: 0 seconds DHCPv6 snooping option 18/37 status: DISABLE DHCPv6 snooping link detection :DISABLE Interface Trusted Filter DHCP ----- FastEthernet0/10 yes DISABLE</pre>	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

15.18 show ipv6 dhcp snooping vlan

	Use this command to display the VLAN with DHCPv6 Snooping function disabled.	
	show ipv6 dhcp snooping vlan	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command is used to display the VLAN with DHCPv6 Snooping function disabled.	
Configuration Examples	The following example displays the VLAN with DHCPv6 Snooping function disabled. FS#show ipv6 dhcp snooping vlan VLAN Name Closed ----- 2 VLAN 2 YES	
	Field	Description
	VLAN	VLAN ID
	NAME	VLAN name
	Close	Indicates whether DHCPv6 Snooping is disabled.
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.19 show ipv6 dhcp snooping binding

	Use this command to display the information of the DHCPv6 Snooping binding database.	
	show ipv6 dhcp snooping binding [<i>mac</i>] [vlan <i>vlan-id</i>] [<i>ipv6-address</i>] [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>mac</i>	Displays the MAC address binding entry.
	<i>vlan_id</i>	Displays the VLAN binding entry.
	<i>ipv6-address</i>	Displays the IPv6 address binding entry.
	<i>interface-id</i>	Displays the interface binding entry.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the information of the DHCP Snooping binding database. <pre>FS# show ipv6 dhcp snooping binding Total number of bindings: 1 NO. MacAddress IPv6 Address Lease(sec) VLAN Interface ----- 1 00d0.f801.0101 2001::10 42368 2 GigabitEthernet 0/1</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

15.20 show ipv6 dhcp snooping prefix

	Use this command to display all user information in the DHCPv6 Snooping prefix list.	
	show ipv6 dhcp snooping prefix [<i>mac</i> vlan <i>vlan-id</i> <i>ipv6-prefix</i> interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>mac</i>	Displays the MAC address prefix entry.
	<i>vlan_id</i>	Displays the VLAN prefix entry.

	<i>ipv6-prefix</i>	Displays the IPv6 address prefix entry.																
	<i>interface-id</i>	Displays the interface prefix entry.																
Defaults	N/A																	
Command Mode	Privileged EXEC mode																	
Usage Guide	N/A																	
Configuration Examples	The following example displays all user information in the DHCPv6 Snooping prefix list. <pre>FS# show ipv6 dhcp snooping prefix</pre> Total number of prefix: 1 <table><thead><tr><th>NO.</th><th>MacAddress</th><th>IPv6 Prefix</th><th>Lease(sec)</th><th>VLAN</th><th>Interface</th></tr></thead><tbody><tr><td>1</td><td>00d0.f801.0101</td><td>2001:2002::</td><td>42368</td><td>2</td><td>GigabitEthernet 0/1</td></tr></tbody></table>						NO.	MacAddress	IPv6 Prefix	Lease(sec)	VLAN	Interface	1	00d0.f801.0101	2001:2002::	42368	2	GigabitEthernet 0/1
NO.	MacAddress	IPv6 Prefix	Lease(sec)	VLAN	Interface													
1	00d0.f801.0101	2001:2002::	42368	2	GigabitEthernet 0/1													
Related Commands	Command			Description														
	N/A			N/A														
Platform Description	N/A																	

15.21 show ipv6 dhcp snooping statistics

	Use this command to display the statistical information of the DHCPv6 packets.	
	show ipv6 dhcp snooping statistics	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the statistical information of the DHCPv6 packets. <pre>FS# show ipv6 dhcp snooping statistics</pre> Packets Processed by DHCPv6 Snooping = 0	

	Packets Dropped Because																		
	Received on untrusted ports	= 0																	
	Relay forward	= 0																	
	No binding entry	= 0																	
	Binding fail	= 0																	
	Unknown packet	= 0																	
	Unknown output interface	= 0																	
	No enough memory	= 0																	
	Admin filter-dhcpv6-pkt	= 0																	
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>Received on untrusted ports</td><td>The discarded server response packets on the untrust port.</td></tr><tr><td>Relay forward</td><td>The packets that have been relayed once are discarded.</td></tr><tr><td>No binding entry</td><td>The binding entries of the release/decline packets are in-existent or error and the packets are discarded.</td></tr><tr><td>Binding fail</td><td>The entry binding fails and the packets are discarded due to a lack of the hardware resources.</td></tr><tr><td>Unknown packet</td><td>The unknown DHCP packets.</td></tr><tr><td>Unknown output interface</td><td>The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.</td></tr><tr><td>No enough memory</td><td>There is no enough memory.</td></tr><tr><td>Admin filter-dhcpv6-pkt</td><td>The filtered DHCPv6 packets configured by the administrator. Use the ipv6 dhcp snooping filter-dhcp-pkt command to filter the packets.</td></tr></table>	Field	Description	Received on untrusted ports	The discarded server response packets on the untrust port.	Relay forward	The packets that have been relayed once are discarded.	No binding entry	The binding entries of the release/decline packets are in-existent or error and the packets are discarded.	Binding fail	The entry binding fails and the packets are discarded due to a lack of the hardware resources.	Unknown packet	The unknown DHCP packets.	Unknown output interface	The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.	No enough memory	There is no enough memory.	Admin filter-dhcpv6-pkt	The filtered DHCPv6 packets configured by the administrator. Use the ipv6 dhcp snooping filter-dhcp-pkt command to filter the packets.
Field	Description																		
Received on untrusted ports	The discarded server response packets on the untrust port.																		
Relay forward	The packets that have been relayed once are discarded.																		
No binding entry	The binding entries of the release/decline packets are in-existent or error and the packets are discarded.																		
Binding fail	The entry binding fails and the packets are discarded due to a lack of the hardware resources.																		
Unknown packet	The unknown DHCP packets.																		
Unknown output interface	The packets on the unknown output interface. The MAC address for the interface is not found or the trust port is not configured.																		
No enough memory	There is no enough memory.																		
Admin filter-dhcpv6-pkt	The filtered DHCPv6 packets configured by the administrator. Use the ipv6 dhcp snooping filter-dhcp-pkt command to filter the packets.																		
Related Commands	Command	Description																	
	N/A	N/A																	
Platform Description	N/A																		

16 ARP-Check Commands

16.1 arp-check

	Use this command to enable the ARP check function on the Layer 2 interface. Use the no form of this command to restore the default setting.	
	arp-check	
	no arp-check	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command mode	Interface configuration mode	
Usage Guide	The ARP check function generates the ARP filtering information according to legal user information, implementing the illegal ARP packet filtering on the network.	
Configuration Examples	This following example enables the APR check function on interface GigabitEthernet 0/1. <pre> FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# arp-check FS(config-if-GigabitEthernet 0/1)# end </pre>	
Related Commands	Command	Description
	show interfaces arp-check list	Displays the ARP check entries.
Platform Description	N/A	

16.2 show interfaces arp-check list

	Use this command to display the ARP check entries on the Layer 2 interface.	
	show { interfaces [interface-type interface-number] } arp-check list	
Parameter Description	Parameter	Description
	<i>interface-type</i>	Wired interface type
	<i>interface-number</i>	Wired interface number

Command mode	Privileged EXEC mode																																								
Usage Guide	Use this command to display the ARP check entries.																																								
Configuration Examples	The following example displays the ARP check entries. <pre>FS(config)#show interfaces arp-check list</pre> <table><thead><tr><th>INTERFACE</th><th>SENDER MAC</th><th>SENDER IP</th><th>POLICY SOURCE</th></tr></thead><tbody><tr><td>GigabitEthernet 0/1</td><td>00D0.F800.0003</td><td>192.168.1.3</td><td>address-bind</td></tr><tr><td>GigabitEthernet 0/1</td><td>00D0.F800.0001</td><td>192.168.1.1</td><td>port-security</td></tr><tr><td>GigabitEthernet 0/4</td><td></td><td>192.168.1.3</td><td>port-security</td></tr><tr><td>GigabitEthernet 0/5</td><td>00D0.F800.0003</td><td>192.168.1.3</td><td>address-bind</td></tr><tr><td>GigabitEthernet 0/7</td><td>00D0.F800.0006</td><td>192.168.1.6</td><td>AAA ip-auth-mode</td></tr><tr><td>GigabitEthernet 0/8</td><td>00D0.F800.0007</td><td>192.168.1.7</td><td>GSN</td></tr></tbody></table> <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>INTERFACE</td><td>Interface name</td></tr><tr><td>SENDER MAC</td><td>Source MAC address</td></tr><tr><td>SENDER IP</td><td>Source IP address</td></tr><tr><td>POLICY SOURCE</td><td>Source of the entry</td></tr></tbody></table>			INTERFACE	SENDER MAC	SENDER IP	POLICY SOURCE	GigabitEthernet 0/1	00D0.F800.0003	192.168.1.3	address-bind	GigabitEthernet 0/1	00D0.F800.0001	192.168.1.1	port-security	GigabitEthernet 0/4		192.168.1.3	port-security	GigabitEthernet 0/5	00D0.F800.0003	192.168.1.3	address-bind	GigabitEthernet 0/7	00D0.F800.0006	192.168.1.6	AAA ip-auth-mode	GigabitEthernet 0/8	00D0.F800.0007	192.168.1.7	GSN	Field	Description	INTERFACE	Interface name	SENDER MAC	Source MAC address	SENDER IP	Source IP address	POLICY SOURCE	Source of the entry
INTERFACE	SENDER MAC	SENDER IP	POLICY SOURCE																																						
GigabitEthernet 0/1	00D0.F800.0003	192.168.1.3	address-bind																																						
GigabitEthernet 0/1	00D0.F800.0001	192.168.1.1	port-security																																						
GigabitEthernet 0/4		192.168.1.3	port-security																																						
GigabitEthernet 0/5	00D0.F800.0003	192.168.1.3	address-bind																																						
GigabitEthernet 0/7	00D0.F800.0006	192.168.1.6	AAA ip-auth-mode																																						
GigabitEthernet 0/8	00D0.F800.0007	192.168.1.7	GSN																																						
Field	Description																																								
INTERFACE	Interface name																																								
SENDER MAC	Source MAC address																																								
SENDER IP	Source IP address																																								
POLICY SOURCE	Source of the entry																																								
Related Commands	Command	Description																																							
	N/A	N/A																																							
Platform Description	N/A																																								

17 DAI Commands

17.1 ip arp inspection trust

	Use this command to configure the L2 port to a trusted port. Use the no form of this command to restore the L2 port to an untrusted port.	
	ip arp inspection trust	
	no ip arp inspection trust	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The L2 port is untrusted.	
Command Mode	Interface configuration mode	
Usage Guide	If it is necessary to make the ARP message received by some interface pass the DAI inspection unconditionally, you can set the interface to a trusted port, indicating that you do not need to check whether the ARP message received by this interface is legal.	
Configuration Examples	The following example sets the gigabitEthernet 0/19 interface as the trusted port. <pre> FS# configure terminal FS(config)# interface gigabitEthernet 0/19 FS(config-if-GigabitEthernet 0/19)# ip arp inspection trust FS(config-if-GigabitEthernet 0/19)# end </pre>	
Related Commands	Command	Description
	show ip arp inspection interface	Displays related DAI information on the interface, including the trust state and rate limit of the interface.
Platform Description	N/A	

17.2 ip arp inspection vlan

	Use this command to configure the DAI function on the VLAN. Use the no form of this command to disable this function.	
	ip arp inspection vlan { vlan-id word }	
	no ip arp inspection vlan { vlan-id word }	

Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
	<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11
Defaults	The DAI function on all VLANs is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	To make this command take effect, you need to enable the ARP Check function first,  Not all ports of the VLAN support the ARP packet detection function. For example, the DHCP Snooping Trust port does not support any security detection, including this function.	
Configuration Examples	The following example detects the received ARP packets on the VLAN1 interfaces: <pre>FS# configure terminal FS(config)# ip arp inspection FS(config)# ip arp inspection vlan 1 FS(config)# end</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

17.3 show ip arp inspection vlan

	Use this command to verify whether the DAI function on the VLAN is enabled.	
	show ip arp inspection vlan [<i>vlan-id</i> <i>word</i>]	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	VLAN ID, ranging from 1 to 4094
	<i>word</i>	String of the VLAN range, such as 1,3-5,7,9-11
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	Use this command to verify whether the DAI function on the VLAN is enabled.											
Configuration Examples	The following example verifies whether the DAI function on the VLAN is enabled: <pre>FS# show ip arp inspection vlan</pre> <table><thead><tr><th>Vlan</th><th>Configuration</th></tr></thead><tbody><tr><td>1</td><td>Active</td></tr></tbody></table> Parameter Description: <table><thead><tr><th>Parameter</th><th>Description</th></tr></thead><tbody><tr><td>Vlan</td><td>VLAN number.</td></tr><tr><td>Configuration</td><td>DAI status (active / inactive)</td></tr></tbody></table>		Vlan	Configuration	1	Active	Parameter	Description	Vlan	VLAN number.	Configuration	DAI status (active / inactive)
Vlan	Configuration											
1	Active											
Parameter	Description											
Vlan	VLAN number.											
Configuration	DAI status (active / inactive)											
Related Commands	Command	Description										
	N/A	N/A										
Platform Description	N/A											

17.4 show ip arp inspection interface

	Use this command to verify whether the interface is a DAI trust interface.													
	show ip arp inspection interface													
Parameter Description	Parameter	Description												
	N/A	N/A												
Defaults	N/A													
Command Mode	Privileged EXEC mode													
Usage Guide	Use this command to verify whether the interface is a DAI trust interface.													
Configuration Examples	The following example verifies the DAI trust state of all : <pre>FS#show ip arp inspection interface</pre> <table><thead><tr><th>Interface</th><th>Trust State</th></tr></thead><tbody><tr><td>-----</td><td>-----</td></tr><tr><td>GigabitEthernet 0/1</td><td>Untrusted</td></tr><tr><td>Default</td><td>Untrusted</td></tr></tbody></table> Parameter Description: <table><thead><tr><th>Parameter</th><th>Description</th></tr></thead><tbody><tr><td>Interface</td><td>Interface name.</td></tr></tbody></table>		Interface	Trust State	-----	-----	GigabitEthernet 0/1	Untrusted	Default	Untrusted	Parameter	Description	Interface	Interface name.
Interface	Trust State													
-----	-----													
GigabitEthernet 0/1	Untrusted													
Default	Untrusted													
Parameter	Description													
Interface	Interface name.													

	Trust State	DAI trust state.	
Related Commands	Command	Description	
	N/A	N/A	
Platform Description	N/A		

18 IP Source Guard Commands

18.1 ip source binding

	Use this command to add static user information to IP source address binding database. Use the no form of this command to delete static user information from IP source address binding database.	
	ip source binding <i>mac-address</i> { vlan <i>vlan-id</i> } <i>ip-address</i> { interface <i>interface-id</i> ip-mac ip-only }	
	no ip source binding <i>mac-address</i> { vlan <i>vlan-id</i> } <i>ip-address</i> { interface <i>interface-id</i> ip-mac ip-only }	
Parameter Description	Parameter	Description
	<i>mac-address</i>	Adds user MAC address statically.
	<i>vlan-id</i>	Adds user VLAN ID statically.
	<i>ip-address</i>	Adds user IP address statically.
	<i>interface-id</i>	Adds user interface ID statically.
	ip-mac	The global binding type is IP+MAC
	ip-only	The global binding type is IP only.
Defaults	No static address is added by default.	
Command Mode	Global configuration mode	
Usage Guide	This command allows specific clients to go through IP source guard detection instead of DHCP. This command is supported on the wired L2 switching port, AP port, and sub interface. This command enables global binding for IP source guard so that specific clients will get detected on all interfaces.  A static IPv6 source binding is valid either on wired interfaces or in global configuration mode.  A new binding will overwrite the old one sharing the same configuration.	
Configuration Examples	The following example adds the interface ID of static users. <pre>FS# configure terminal FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface GigabitEthernet 0/1 FS(config)# end</pre> The following example adds static user information based on IP-MAC binding. <pre>FS# configure terminal FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac FS(config)# end</pre> The following example adds static user information based on IP binding. <pre>FS# configure terminal</pre>	

	<pre>FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only FS(config)# end</pre>	
Related Commands	Command	Description
	show ip source binding	Displays the binding information of IP source address and database.
Platform Description	N/A	

18.2 ip verify source

	Use this command to enable IP Source Guard function on the interface. Use the no form of this command to restore the default setting.	
	ip verify source [port-security]	
	no ip verify source	
Parameter Description	Parameter	Description
	port-security	Configures IP Source Guard to do IP+MAC-based detection.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	This command enables IP Source Guard function on the interface to do IP-based or IP+MAC-based detection. This command is supported on the wired L2 switching port, AP port, and sub interface  IP Source Guard takes effect only on DHCP Snooping untrusted port. In other words, IP Source Guard does not take effect when configuring it on Trust port or the port which is not controlled by DHCP Snooping.	
Configuration Examples	The following example enables IP-based IP Source Guard function. <pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip verify source FS(config-if)# end</pre> The following example enables IP+MAC-based IP Source Guard function. <pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)# ip verify source port-security FS(config-if)# end</pre>	

Related Commands	Command	Description
	show ip verify source	Displays user filtering entry of IP Source Guard.
Platform Description	N/A	

18.3 ip verify source exclude-vlan

	Use this command to exclude a VLAN from the IP source guard configuration on the port. Use the no form of this command to restore the function.	
	ip verify source exclude-vlan <i>vlan-id</i>	
	no ip verify source exclude-vlan <i>vlan-id</i>	
Parameter Description	Parameter	Description
	<i>vlan-id</i>	The ID of VLAN excluded from the IP source guard configuration.
Defaults	This function is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	● This command is used to exclude a VLAN from the IP source guard configuration. IP packets in this VLAN are forwarded without being checked and filtered. ● Once the IP source guard function is disabled, the excluded VLAN is cleared automatically. ● This command is supported on the wired L2 switching port, AP port, and sub interface.  Only when the IP source guard configuration is enabled on the port can a VLAN be excluded.	
Configuration Examples	The following example configuration configures the IP source guard configuration for the port and excludes a VLAN. <pre> FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ip verify source FS(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1 FS(config-if)# end </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

18.4 show ip source binding

	Use this command to display the binding information of IP source addresses and database.	
	show ip source binding [<i>ip-address</i>] [<i>mac-address</i>] [dhcp-snooping] [static] [vlan <i>vlan-id</i>] [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Displays user binding information of corresponding IP.
	<i>mac-address</i>	Displays user binding information of corresponding MAC.
	dhcp-snooping	Displays binding information of dynamic user.
	static	Displays binding information of static user.
	<i>vlan-id</i>	Displays user binding information of corresponding VLAN.
	<i>interface-id</i>	Displays user binding information of corresponding interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the binding information of IP source guard addresses and database. <pre> FS# show ip source binding static FS#show ip source binding static Total number of bindings: 5 NO. MACADDRESS IPADDRESS LEASE(SEC) TYPE VLAN INTERFACE ----- 1 0001.0002.0001 1.2.3.2 Infinite Static 1 Global 2 0001.0002.0002 1.2.3.3 Infinite Static 1 GigabitEthernet 0/5 3 0001.0002.0003 1.2.3.4 Infinite Static 1 Global 4 0001.0002.0004 1.2.3.5 Infinite Static 1 Global </pre>	
Related Commands	Command	Description
	ip source binding	Sets the binding static user.
Platform Description	N/A	

18.5 show ip verify source

	Use this command to display user filtering entry of IP Source Guard.
	show ip verify source [interface <i>interface-id</i>]

Parameter Description	Parameter	Description
	<i>interface-id</i>	Displays user filtering entry of corresponding interface.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	If IP Source Guard is not enabled on the corresponding interface, the printing information will be shown on the terminal as: "IP source guard is not configured on the interface FastEthernet 0/10" Now, IP Source Guard supports the following filtering modes: inactive-restrict-off: the IP Source Guard is disabled on bound interfaces. inactive--not-apply: the IP Source Guard cannot adds bound entries into filtering entries for system errors. active: the IP Source Guard is active.	
Configuration Examples	The following example displays user filtering entry of IP Source Guard. <pre> FS # show ip verify source Total number of bindings: 7 NO. INTERFACE FILTERTYPE FILTERSTATUS IPADDRESS MACADDRESS VLAN TYPE ----- 1 Global IP+MAC Inactive-not-apply 192.168.0.127 0001.0002.0003 1 Static 2 GigabitEthernet 0/5 IP-ONLY Active 1.2.3.4 0001.0002.0004 1 DHCP-Snooping 3 Global IP-ONLY Active 1.2.3.7 0001.0002.0007 1 Static 4 Global IP+MAC Active 1.2.3.6 0001.0002.0006 1 Static 5 GigabitEthernet 0/1 UNSET Inactive-restrict-off 1.2.3.9 0001.0002.0009 1 DHCP-Snooping 6 GigabitEthernet 0/5 IP-ONLY Active Deny-All </pre>	
Related Commands	Command	Description
	ip verify source	Sets IP Source Guard on the interface.
Platform Description	N/A	

19 IPv6 Source Guard Commands

19.1 ipv6 source binding

	Use this command to configure a static IPv6 source binding. Use the no form of this command to delete a static IPv6 source binding.	
	ipv6 source binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ipv6-address</i> { interface <i>interface-id</i> ip-mac ip-only }	
	no ipv6 source binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ipv6-address</i> { interface <i>interface-id</i> ip-mac ip-only }	
Parameter Description	Parameter	Description
	<i>mac-address</i>	MAC address
	<i>vlan-id</i>	VLAN ID
	<i>ipv6-address</i>	IPv6 address
	<i>interface-id</i>	Wired interface ID
	ip-mac	IPv6-MAC binding
	ip-only	IPv6-only binding
Defaults	No static IPv6 source binding is configured by default.	
Command Mode	Global configuration mode	
Usage Guide	● Use this command to exempt trusted hosts from IPv6 source guard. ● This command is supported only on Layer 2 ports, aggregate ports and encapsulated sub interfaces.  A static IPv6 source binding is valid either on wired interfaces or in global configuration mode.  A new binding will overwrite the old one sharing the same configuration.	
Configuration Examples	The following example configures static IPv6 source bindings on GigabitEthernet 0/1. <pre>FS# configure terminal FS(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 interface GigabitEthernet 0/1 FS(config)# end</pre> The following example configures a static IPv6-MAC binding. <pre>FS# configure terminal FS(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-mac FS(config)# end</pre> The following example configures a static IPv6-only binding. <pre>FS# configure terminal FS(config)# ipv6 source binding 0000.0000.0001 vlan 1 1::1 ip-only FS(config)# end</pre>	

Platform Description	N/A

19.2 ipv6 verify source

	Use this command to enable IPv6 source guard. Use the no form of this command to restore the default setting.	
	ipv6 verify source [port-security]	
	no ipv6 verify source	
Parameter Description	Parameter	Description
	port-security	Enables source IPv6-MAC filtering.
Defaults	IPv6 source guard is disabled by default.	
Command Mode	Interface configuration mode	
Usage Guide	Use this command to enable IPv6 source guard with source IPv6 filtering or source IPv6-MAC filtering. This command is supported only on Layer 2 ports, aggregate ports and encapsulated sub interface.  Currently, the IPv6 source guard feature of FS devices filters traffic based on the DHCPv6 Snooping database or on manually configured IPv6 source bindings. A port with only IPv6 source guard enabled cannot realize normal network access for connected hosts.	
Configuration Examples	The following example enables IPv6 source guard based on source IPv6 filtering. <pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/1 FS(config-if-GigabitEthernet 0/1)# ipv6 verify source FS(config-if)# end</pre> The following example enables IPv6 source guard based on source IPv6-MAC filtering. <pre>FS# configure terminal FS(config)# interface GigabitEthernet 0/2 FS(config-if-GigabitEthernet 0/2)# ipv6 verify source port-security FS(config-if)# end</pre>	
Platform Description	N/A	

19.3 show ipv6 source binding

	Use this command to display the IPv6 source binding database. show ipv6 source binding [<i>ipv6-address</i>] [<i>mac-address</i>] [dhcp-snooping] [static] [vlan <i>vlan-id</i>] [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>ipv6-address</i>	Displays the source IPv6 address bindings.
	<i>mac-address</i>	Displays the source MAC address bindings.
	dhcp-snooping	Displays the DHCP snooping bindings.
	static	Displays the static IPv6 source bindings.
	<i>vlan-id</i>	Displays the VLAN bindings.
	<i>interface-id</i>	Displays the interface bindings.
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the IPv6 source binding database. <pre> FS# show ipv6 source binding Total number of bindings: 7 NO. Filter Type Filter Status IPv6 Address MACAddress VLAN Type Interface ----- 1 IPv6+MAC Inactive-system-error 2000::127 0001.0002.0003 1 Static Global 2 IPv6-ONLY Active 2008::4 0001.0002.0004 1 DHCPv6-Snooping GigabitEthernet 0/5 3 IPv6-ONLY Active 2008::7 0001.0002.0007 1 Static Global 4 IPv6+MAC Active 2008::1 0001.0002.0006 1 Static Global 5 UNSET Inactive-restrict-off 2008::9 0001.0002.0009 1 DHCPv6-Snooping GigabitEthernet 0/1 6 IPv6-ONLY Active Deny-All GigabitEthernet 0/5 </pre>	
Platform Description	N/A	

20 Anti-ARP Spoofing Commands

20.1 anti-arp-spoofing ip

	Use this command to enable anti-ARP spoofing. Use the no form of this command to disable this function.	
	anti-arp-spoofing ip <i>ip-address</i>	
	no anti-arp-spoofing ip <i>ip-address</i>	
Parameter Description	Parameter	Description
	<i>ip-address</i>	Gateway IP address
Defaults	The anti-ARP spoofing function is disabled by default.	
Command Mode	Interface configuration mode/Wireless security configuration mode	
Usage Guide	This command is used to enable anti-ARP spoofing on only L2 interfaces. This command is used on AC/AP only in wireless security configuration mode. Use the show anti-arp-spoofing command to display the configuration.	
Configuration Examples	The following example enables anti-ARP spoofing. FS(config)#interface fastEthernet 0/1 FS(config-if)#anti-arp-spoofing ip 192.168.1.1	
Related Commands	Command	Description
	show anti-arp-spoofing	Displays the anti-ARP spoofing configuration.
Platform Description	N/A	

20.2 show anti-arp-spoofing

	Use this command to display the anti-ARP spoofing configuration on all interfaces.	
	show anti-arp-spoofing	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	

Command Mode	Global configuration mode																								
Usage Guide	This command is used to display the anti-ARP spoofing configuration on all interfaces.																								
Configuration Examples	The following example displays the anti-ARP-spoofing configuration on all interfaces. <pre>FS#show anti-arp-spoofing</pre> <table><thead><tr><th>NO</th><th>PORT</th><th>IP</th><th>STATUS</th></tr></thead><tbody><tr><td colspan="4">-----</td></tr><tr><td>1</td><td>Gi0/1</td><td>192.168.1.1</td><td>active</td></tr></tbody></table> Field Description <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>NO</td><td>Order number</td></tr><tr><td>PORT</td><td>Port number</td></tr><tr><td>IP</td><td>Gateway IP</td></tr><tr><td>STATUS</td><td>Anti-ARP spoofing status</td></tr></tbody></table>			NO	PORT	IP	STATUS	-----				1	Gi0/1	192.168.1.1	active	Field	Description	NO	Order number	PORT	Port number	IP	Gateway IP	STATUS	Anti-ARP spoofing status
NO	PORT	IP	STATUS																						

1	Gi0/1	192.168.1.1	active																						
Field	Description																								
NO	Order number																								
PORT	Port number																								
IP	Gateway IP																								
STATUS	Anti-ARP spoofing status																								
Related Commands	Command	Description																							
	anti-arp-spoofing ip	Configures anti-ARP spoofing.																							
Platform Description	N/A																								

21 NFPP Commands

21.1 arp-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the no or default form of this command to restore the default setting.	
	arp-guard attack-threshold { per-src-ip per-src-mac per-port } pps	
	no arp-guard attack-threshold { per-src-ip per-src-mac per-port }	
	default arp-guard attack-threshold { per-src-ip per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	pps	Sets the attack threshold, in the range from 1 to 19,999 in unit of pps.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode.	
Usage Guide	The attack threshold shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the global attack threshold. <pre> FS(config)# nfpp FS(config-nfpp)# arp-guard attack-threshold per-src-ip 2 FS(config-nfpp)# arp-guard attack-threshold per-src-mac 3 FS(config-nfpp)# arp-guard attack-threshold per-port 50 </pre>	
Related Commands	Command	Description
	nfpp arp-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host.
	clear nfpp arp-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.2 arp-guard enable

	Use this command to enable the anti-ARP guard function globally. Use the no or default form of this command to restore the default setting.	
	arp-guard enable	
	no arp-guard enable	
	default arp-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	NFPP configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example enables the anti-ARP guard function globally. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard enable</pre>	
Related Commands	Command	Description
	nfpp arp-guard enable	Enables the anti-ARP attack on the interface.
	show nfpp arp-guard summary	Displays the configuration.
Platform Description	N/A	

21.3 arp-guard isolate-period

	Use this command to set the arp-guard isolate time globally. Use the no or default form of this command to restore the default setting.	
	arp-guard isolate-period { seconds permanent }	
	no arp-guard isolate-period	
	default arp-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate time. The value is 0, or in the range from 30 to 86400 in the unit of seconds.
	permanent	Permanent isolation.

Defaults	The default isolate time is 0, which means no isolation.						
Command Mode	NFPP configuration mode.						
Usage Guide	N/A						
Configuration Examples	The following example sets the arp-guard isolate time globally to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard isolate-period 180</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>nfpp arp-guard isolate-period</td><td>Sets the isolate time on the interface.</td></tr> <tr> <td>show nfpp arp-guard summary</td><td>Displays the configuration.</td></tr> </table>	Command	Description	nfpp arp-guard isolate-period	Sets the isolate time on the interface.	show nfpp arp-guard summary	Displays the configuration.
Command	Description						
nfpp arp-guard isolate-period	Sets the isolate time on the interface.						
show nfpp arp-guard summary	Displays the configuration.						
Platform Description	N/A						

21.4 arp-guard isolate-forwarding enable

	Use this command to enable packet forwarding through NFPP isolation. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	arp-guard isolate-forwarding enable	
	no arp-guard isolate-forwarding enable	
	default arp-guard isolate-forwarding enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables packet forwarding through NFPP isolation. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard isolate-forwarding enable</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

21.5 arp-guard monitored-host-limit

	Use this command to set the maximum monitored host number. Use the no or default form of this command to restore the default setting.	
	arp-guard monitored-host-limit <i>number</i>	
	no arp-guard monitored-host-limit	
	default arp-guard monitored-host-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20000.	
Command Mode	NFPP configuration mode	
Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.	
Configuration Examples	The following example sets the maximum monitored host number to 200. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard monitored-host-limit 200</pre>	
Related Commands	Command	Description
	show nfpp arp-guard summary	Displays the configuration.
Platform Description	N/A	

21.6 arp-guard monitor-period

	Use this command to configure the arp guard monitor time. Use the no or default form of this command to restore the default setting.	
	arp guard monitor-period <i>seconds</i>	
	no arp-guard monitor-period	
	default arp-guard monitor-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.
Defaults	The default is 600.	
Command Mode	NFPP configuration mode	
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.	
Configuration Examples	The following example sets the arp guard monitor time to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard monitor-period 180</pre>	
Related Commands	Command	Description
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host list.
	clear nfpp arp-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.7 arp-guard rate-limit

	Use this command to set the arp guard rate limit. Use the no or default form of this command to restore the default setting.	
	arp-guard rate-limit { per-src-ip per-src-mac per-port } <i>pps</i>	
	no arp-guard rate-limit { per-src-ip per-src-mac per-port }	
	default arp-guard rate-limit { per-src-ip per-src-mac per-port }	

Parameter Description	Parameter	Description
	per-src-ip	Sets the rate limit for each source IP address.
	per-src-mac	Sets the rate limit for each source MAC address.
	per-port	Sets the rate limit for each port.
	<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the arp guard rate limit. <pre> FS(config)# nfpp FS(config-nfpp)# arp-guard rate-limit per-src-ip 2 FS(config-nfpp)# arp-guard rate-limit per-src-mac 3 FS(config-nfpp)# arp-guard rate-limit per-port 50 </pre>	
Related Commands	Command	Description
	nfpp arp-guard policy	Sets the rate limit and the attack threshold.
	show nfpp arp-guard summary	Displays the configuration.
Platform Description	N/A	

21.8 arp-guard ratelimit-forwarding enable

	Use this command to set the port based arp guard rate limit. Use the no form of this command to disable this function. Use the default form of this command to restore the default setting.	
	arp-guard ratelimit-forwarding enable	
	no arp-guard ratelimit-forwarding enable	
	default arp-guard ratelimit-forwarding enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	

Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the port based arp guard rate limit. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard ratelimit-forwarding enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

21.9 arp-guard scan-threshold

	Use this command to set the global scan threshold. Use the no or default form of this command to restore the default setting.	
	arp-guard scan-threshold <i>pkt-cnt</i>	
	no arp-guard scan-threshold	
	default arp-guard scan-threshold	
Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999 in the unit of seconds.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	The scanning may occur on the condition that: ● More than 15 packets are received within 10 seconds; ● The source MAC address for the link layer is constant while the source IP address is uncertain; ● The source MAC and IP address for the link layer is constant while the destination IP address is uncertain.	
Configuration Examples	The following example sets the global scan threshold to 20pps. <pre>FS(config)# nfpp FS(config-nfpp)# arp-guard scan-threshold 20</pre>	

Related Commands	Command	Description
	nfpp arp-guard scan-threshold	Sets the scan threshold on the port.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard scan	Displays the ARP guard scan table.
	clear nfpp arp-guard scan	Clears the ARP guard scan table.
Platform Description	N/A	

21.10 clear nfpp arp-guard hosts

	Use this command to clear the monitored host isolation.	
	clear nfpp arp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i> <i>mac-address</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>ip-address</i>	Sets the IP address.
	<i>mac-address</i>	Sets the MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears the monitored host isolation.	
	FS# clear nfpp arp-guard hosts vlan 1 interface g0/1	
Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	nfpp arp-guard policy	Sets the limit threshold and attack threshold.
	show nfpp arp-guard hosts	Displays the monitored host.
Platform Description	N/A	

21.11 clear nfpp arp-guard scan

	Use this command to clear ARP scanning table.

	clear nfpp arp-guard scan	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears ARP scanning table. FS# clear nfpp arp-guard scan	
Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	nfpp arp-guard policy	Sets the attack threshold.
	show nfpp arp-guard scan	Displays the ARP scanning table.
Platform Description	N/A	

21.12 clear nfpp define name hosts

	Use this command to clear the monitored hosts. If the host is isolated, you need to release it.	
	clear nfpp define <i>name</i> hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>] [<i>mac-address</i>] [<i>ipv6-address</i>]	
Parameter Description	Parameter	Description
	<i>name</i>	Defines guard name
	<i>vid</i>	VLAN ID
	<i>interface-id</i>	Interface name
	<i>ip-address</i>	IP address
	<i>mac</i>	MAC address
	<i>ipv6-address</i>	IPv6 address
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	Use this command without the parameter to clear all monitored hosts in the self-defined range.	
Configuration Examples	The following example clears the monitored hosts. <pre>FS# clear nfpp define tcp hosts vlan 1 interface g 0/1</pre>	
Related Commands	Command	Description
	show nfpp define hosts	Displays the isolated hosts.
Platform Description	N/A	

21.13 clear nfpp dhcp-guard hosts

	Use this command to clear the DHCP monitored hosts, that is, release them from isolation.	
	clear nfpp dhcp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>mac-address</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>mac-address</i>	Sets the MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command without the parameter to clear all monitored hosts.	
Configuration Examples	The following example clears the DHCP monitored hosts. <pre>FS# clear nfpp dhcp-guard hosts vlan 1 interface g0/1</pre>	
Related Commands	Command	Description
	dhcp-guard attack-threshold	Sets the global attack threshold.
	nfpp dhcp-guard policy	Sets the limit threshold and attack threshold.
	show nfpp dhcp-guard hosts	Displays the monitored host.
Platform Description	N/A	

21.14 clear nfpp dhcpv6-guard hosts

	Use this command to clear the DHCPv6 monitored host isolation.	
	clear nfpp dhcpv6-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>mac-address</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>mac-address</i>	Sets the MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command without the parameter to clear all monitored hosts	
Configuration Examples	The following example clears the DHCPv6 monitored hosts. <pre>FS# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1</pre>	
Related Commands	Command	Description
	dhcpv6-guard attack-threshold	Sets the global attack threshold.
	nfpp dhcpv6-guard policy	Sets the limit threshold and attack threshold.
	show nfpp dhcpv6-guard hosts	Displays the monitored host.
Platform Description	N/A	

21.15 clear nfpp icmp-guard hosts

	Use this command to clear the ICMP monitored hosts.	
	clear nfpp icmp-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>ip-address</i>	Sets the IP address.
Defaults	N/A	
Command	Privileged EXEC mode	

Mode		
Usage Guide	Use this command without the parameter to clear all monitored hosts.	
Configuration Examples	The following example clears the ICMP monitored hosts. FS# clear nfpp icmp-guard hosts vlan 1 interface g0/1	
Related Commands	Command	Description
	icmp-guard attack-threshold	Sets the global attack threshold.
	nfpp icmp-guard policy	Sets the limit threshold and attack threshold.
	show nfpp icmp-guard hosts	Displays the monitored host.
Platform Description	N/A	

21.16 clear nfpp ip-guard hosts

	Use this command to clear the monitored host isolation.	
	clear nfpp ip-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
	<i>ip-address</i>	Sets the IP address.
Defaults	N/A.	
Command Mode	Privileged EXEC mode	
Usage Guide	Use this command without the parameter to clear all monitored hosts.	
Configuration Examples	The following example clears the monitored host isolation. FS# clear nfpp ip-guard hosts vlan 1 interface g0/1	
Related Commands	Command	Description
	ip-guard attack-threshold	Sets the global attack threshold.
	nfpp ip-guard policy	Sets the limit threshold and attack threshold.
	show nfpp ip-guard hosts	Displays the monitored host.
Platform Description	N/A	

21.17 clear nfpp nd-guard hosts

	Use this command to remove the speed limit on the monitored host. clear nfpp nd-guard hosts [vlan <i>vid</i>] [interface <i>interface-id</i>]	
Parameter Description	Parameter	Description
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command without any parameter is used to remove speed limit on all monitored hosts.	
Configuration Examples	The following example removes speed limit on interface g0/1 in VLAN 1. FS# clear nfpp nd-guard hosts vlan 1 interface g0/1	
Prompt Messages	N/A	
Platform Description	N/A	

21.18 clear nfpp log

	Use this command to clear the NFPP log buffer area.	
	clear nfpp log	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example clears the NFPP log buffer area. FS# clear nfpp log	

Related Commands	Command	Description
	show nfpp log	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

21.19 define

	Use this command to define the anti-attack type. Use the no or default form of this command to restore the default setting.	
	define <i>name</i>	
	no define <i>name</i>	
	default define <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type
Defaults	N/A	
Command Mode	NFPP configuration mode	
Usage Guide	Use this command to define the anti-attack type.	
Configuration Examples	The following example creates the user-defined anti-attack type. <pre>FS(config)# nfpp FS(config-nfpp)# define tcp FS(config-nfpp-define)#</pre>	
Related Commands	Command	Description
	show nfpp define summary	Displays the defined anti-attack configuration.
Platform Description	N/A	

21.20 define name enable

	Use this command to enable the user-defined anti-attack globally. Use the no or default form of this command to restore the default setting.	
	define <i>name</i> enable	

	no define name enable	
	default define name enable	
Parameter Description	Parameter	Description
	<i>name</i>	Defines guard name.
Defaults	This function is disabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	This command takes effect only after the match, rate-limit and attack-threshold have been configured.	
Configuration Examples	The following example enabled the user-defined anti-attack globally. <pre>FS(config)# nfpp FS(config-nfpp)#define tcp enable</pre>	
Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration
Platform Description	N/A	

21.21 dhcp-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the no or default form of this command to restore the default setting.	
	dhcp-guard attack-threshold { per-src-mac per-port } pps	
	no dhcp-guard attack-threshold { per-src-mac per-port }	
	default dhcp-guard attack-threshold { per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in pps. The valid range is 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command	NFPP configuration mode	

Mode		
Usage Guide	N/A	
Configuration Examples	The following example sets the global attack threshold. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15 FS(config-nfpp)# dhcp-guard attack-threshold per-port 200</pre>	
Related Commands	Command	Description
	nfpp dhcp-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp dhcp-guard summary	Displays the configuration.
	show nfpp dhcp-guard hosts	Displays the monitored host list.
	clear nfpp dhcp-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.22 dhcp-guard enable

	Use this command to enable the DHCP anti-attack function. Use the no or default form of this command to restore the default setting.	
	dhcp-guard enable	
	no dhcp-guard enable	
	default dhcp-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the DHCP anti-attack function. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard enable</pre>	

Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

21.23 dhcp-guard isolate-period

	Use this command to set the isolate time globally. Use the no or default form of this command to restore the default setting.	
	dhcp-guard isolate-period { <i>seconds</i> permanent }	
	no dhcp-guard isolate-period	
	default dhcp-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation.
Defaults	The default isolate time is 0, which means no isolation.	
Command Mode	NFPP configuration mode	
Usage Guide	The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.	
Configuration Examples	The following example sets the isolate time globally to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard isolate-period 180</pre>	
Related Commands	Command	Description
	nfpp dhcp-guard isolate-period	Sets the isolate time on the interface.
	show nfpp dhcp-guard summary	Displays the configuration.
Platform Description	N/A	

21.24 dhcp-guard monitored-host-limit

	Use this command to set the maximum monitored host number.

	Use the no or default form of this command to restore the default setting.	
	dhcp-guard monitored-host-limit <i>number</i>	
	no dhcp-guard monitored-host-limit	
	default dhcp-guard monitored-host-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20,000.	
Command Mode	NFPP configuration mode	
Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.	
Configuration Examples	The following example sets the maximum monitored host number to 200. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard monitored-host-limit 200</pre>	
Related Commands	Command	Description
	show nfpp dhcp-guard summary	Displays the configuration.
Platform Description	N/A	

21.25 dhcp-guard monitor-period

	Use this command to configure the monitor time.	
	Use the no or default form of this command to restore the default setting.	
	dhcp-guard monitor-period <i>seconds</i>	
	no dhcp-guard monitor-period	
	default dhcp-guard monitor-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.

Defaults	The default is 600 seconds.								
Command Mode	NFPP configuration mode								
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.								
Configuration Examples	The following example sets the monitor time to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard monitor-period 180</pre>								
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>show nfpp dhcp-guard summary</td><td>Displays the configuration.</td></tr> <tr> <td>show nfpp dhcp-guard hosts</td><td>Displays the monitored host list.</td></tr> <tr> <td>clear nfpp dhcp-guard hosts</td><td>Clears the isolated host.</td></tr> </table>	Command	Description	show nfpp dhcp-guard summary	Displays the configuration.	show nfpp dhcp-guard hosts	Displays the monitored host list.	clear nfpp dhcp-guard hosts	Clears the isolated host.
Command	Description								
show nfpp dhcp-guard summary	Displays the configuration.								
show nfpp dhcp-guard hosts	Displays the monitored host list.								
clear nfpp dhcp-guard hosts	Clears the isolated host.								
Platform Description	N/A								

21.26 dhcp-guard rate-limit

	Use this command to set the rate-limit threshold globally. Use the no or default form of this command to restore the default setting.	
	dhcp-guard rate-limit { per-src-mac per-port } pps	
	no dhcp-guard rate-limit { per-src-mac per-port }	
	default dhcp-guard rate-limit { per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-mac	Sets the rate limit for each source MAC address.
	per-port	Sets the rate limit for each port.
	<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command	NFPP configuration mode	

Mode		
Usage Guide	N/A	
Configuration Examples	The following example sets the rate-limit threshold globally. <pre>FS(config)# nfpp FS(config-nfpp)# dhcp-guard rate-limit per-src-mac 8 FS(config-nfpp)# dhcp-guard rate-limit per-port 100</pre>	
Related Commands	Command	Description
	nfpp dhcp-guard policy	Sets the rate limit and the attack threshold.
	show nfpp dhcp-guard summary	Displays the configuration.
Platform Description	N/A	

21.27 dhcpv6-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the no or default form of this command to restore the default setting.	
	dhcpv6-guard attack-threshold { per-src-mac per-port } pps	
	no dhcpv6-guard attack-threshold { per-src-mac per-port }	
	default dhcpv6-guard attack-threshold { per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in the range is from 1 to 19,999 pps.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A.	
Configuration Examples	The following example sets the global attack threshold. <pre>FS(config)# nfpp FS(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15 FS(config-nfpp)# dhcpv6-guard attack-threshold per-port 200</pre>	

Related Commands	Command	Description
	nfpp dhcpv6-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp dhcpv6-guard summary	Displays the configuration.
	show nfpp dhcpv6-guard hosts	Displays the monitored host list.
	clear nfpp dhcpv6-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.28 dhcpv6-guard enable

	Use this command to enable the DHCPv6 anti-attack function. Use the no or default form of this command to restore the default setting.	
	dhcpv6-guard enable	
	no dhcpv6-guard enable	
	default dhcpv6-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the DHCPv6 anti-attack function globally. <pre>FS(config)# nfpp FS(config-nfpp)# dhcpv6-guard enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

21.29 dhcpv6-guard monitored-host-limit

	Use this command to set the maximum monitored host number. Use the no or default form of this command to restore the default setting.	
	dhcpv6-guard monitored-host-limit <i>number</i>	
	no dhcpv6-guard monitored-host-limit	
	default dhcpv6-guard monitored-host-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20,000.	
Command Mode	NFPP configuration mode	
Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20000 monitored hosts to remind the administrator.	
Configuration Examples	The following example sets the maximum monitored host number to 200. <pre>FS(config)# nfpp FS(config-nfpp)# dhcpv6-guard monitored-host-limit 200</pre>	
Related Commands	Command	Description
	show nfpp dhcpv6-guard summary	Displays the configuration.
Platform Description	N/A	

21.30 dhcpv6-guard monitor-period

	Use this command to configure the monitor time. Use the no or default form of this command to restore the default setting.	
	dhcpv6-guard monitor-period <i>seconds</i>	
	no dhcpv6-guard monitor-period	
	default dhcpv6-guard monitor-period	

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.
Defaults	The default is 600 seconds.	
Command Mode	NFPP configuration mode	
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.	
Configuration Examples	The following example sets the monitor time to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# dhcpv6-guard monitor-period 180</pre>	
Related Commands	Command	Description
	show nfpp dhcpv6-guard summary	Displays the configuration.
	show nfpp dhcpv6-guard hosts	Displays the monitored host list.
	clear nfpp dhcpv6-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.31 dhcpv6-guard rate-limit

	Use this command to set the rate-limit threshold globally. Use the no or default form of this command to restore the default setting.	
	dhcpv6-guard rate-limit { per-src-mac per-port } pps	
	no dhcpv6-guard rate-limit { per-src-mac per-port }	
	default dhcpv6-guard rate-limit { per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-mac	Sets the rate limit for each source MAC address.
	per-port	Sets the rate limit for each port.
	<i>pps</i>	Sets the rate limit, in the range from 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	

Command Mode	NFPP configuration mode						
Usage Guide	N/A						
Configuration Examples	The following example sets the rate-limit threshold globally. <pre>FS(config)# nfpp FS(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8 FS(config-nfpp)# dhcpv6-guard rate-limit per-port 100</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>nfpp dhcpv6-guard policy</td><td>Sets the rate limit and the attack threshold.</td></tr> <tr> <td>show nfpp dhcpv6-guard summary</td><td>Displays the configuration.</td></tr> </table>	Command	Description	nfpp dhcpv6-guard policy	Sets the rate limit and the attack threshold.	show nfpp dhcpv6-guard summary	Displays the configuration.
Command	Description						
nfpp dhcpv6-guard policy	Sets the rate limit and the attack threshold.						
show nfpp dhcpv6-guard summary	Displays the configuration.						
Platform Description	N/A						

21.32 global-policy

	Use this command to set the rate-limit threshold and attack threshold based on the host or port. Use the no or default form of this command to restore the default setting.	
	global-policy { per-src-mac per-src-ip per-port } <i>rate-limit-pps attack-threshold-pps</i>	
	no global-policy { per-src-mac per-src-ip per-port }	
	default global-policy { per-src-mac per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Performs the rate statistics based on the source IP / VID and port.
	per-src-mac	Performs the rate statistics based on the source MAC / VID and port.
	per-port	Performs the rate statistics based on each physical port of receiving the packets.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold.
	<i>attack-threshold-pps</i>	Sets the attack threshold.
Defaults	By default, no rate-limit threshold and attack threshold is configured. To enable self-defined anti-attack, these two parameters must be set.	
Command Mode	NFPP define configuration mode	
Usage Guide	To create a user-defined anti-attack type, the classification rule for the rate statistics must be specified, that is,	

	recognize the host based on the source IP address/ source MAC address for the user-defined packets rate statistics based on the user / port and specify the rate-limit threshold and attack threshold for each classification. The rate-limit threshold shall be equal to or greater than the attack threshold. If the rate is greater than the rate-limit threshold, the packets that meet this classification rule will be discarded. If the rate exceeds the attack threshold, the user will be regarded as an attacker. The log will be printed and the trap will be sent.	
Configuration Examples	The following example sets the rate-limit threshold and attack threshold based on the host or port. <pre>FS(config)# nfpp FS(config-nfpp)# nfpp define tcp FS(config-nfpp-define)# global-policy per-src-ip 10 20 FS(config-nfpp-define)# global-policy per-port 100 200</pre>	
Related Commands	Command	Description
	nfpp define <i>name</i> policy	Sets the rate-limit threshold and attack threshold.
	show nfpp define summary	Displays the user-defined anti-attack configuration
Platform Description	N/A	

21.33 icmp-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.	
	Use the no or default form of this command to restore the default setting.	
	icmp-guard attack-threshold { per-src-ip per-port } pps	
	no icmp-guard attack-threshold { per-src-ip per-port }	
	default icmp-guard attack-threshold { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in the range from 1 to 19,999 in the unit of pps.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration	The following example sets the global attack threshold.	

Examples	FS(config)# nfpp FS(config-nfpp)# icmp-guard attack-threshold per-src-ip 600 FS(config-nfpp)# icmp-guard attack-threshold per-port 1200	
Related Commands	Command	Description
	nfpp icmp-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp icmp-guard summary	Displays the configuration.
	show nfpp icmp-guard hosts	Displays the monitored host list.
	clear nfpp icmp-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.34 icmp-guard enable

	Use this command to enable the ICMP anti-attack function. Use the no or default form of this command to restore the default setting.	
	icmp-guard enable	
	no icmp-guard enable	
	default icmp-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the ICMP anti-attack function globally. FS(config)# nfpp FS(config-nfpp)# icmp-guard enable	
Related Commands	Command	Description
	nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.
	show nfpp icmp-guard summary	Displays the configuration.

Platform	N/A
Description	

21.35 icmp-guard isolate-period

	Use this command to set the isolate time globally. Use the no or default form of this command to restore the default setting.	
	icmp-guard isolate-period { <i>seconds</i> permanent }	
	no icmp-guard isolate-period	
	default icmp-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate time. The value is in the range is 0 or from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation.
Defaults	The default isolate time is 0, which means no isolation.	
Command Mode	NFPP configuration mode	
Usage Guide	The isolate period can be configured globally or based on the interface. For one interface, if the isolate period is not set based on the interface, the global value shall be adopted; or the interface-based isolate period shall be adopted.	
Configuration Examples	The following example sets the isolate time globally to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# icmp-guard isolate-period 180</pre>	
Related Commands	Command	Description
	nfpp icmp-guard isolate-period	Sets the isolate time on the interface.
	show nfpp icmp-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.36 icmp-guard monitored-host-limit

	Use this command to set the maximum monitored host number. Use the no or default form of this command to restore the default setting.	
	icmp-guard monitored-host-limit <i>number</i>	
	no icmp-guard monitored-host-limit	
	default icmp-guard monitored-host-limit	

Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20,000.	
Command Mode	NFPP configuration mode	
Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that %NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.	
Configuration Examples	The following example sets the maximum monitored host number to 200. <pre>FS(config)# nfpp FS(config-nfpp)# icmp-guard monitored-host-limit 200</pre>	
Related Commands	Command	Description
	show nfpp icmp-guard summary	Displays the configuration.
Platform Description	N/A	

21.37 icmp-guard monitor-period

	Use this command to configure the monitor time. Use the no or default form of this command to restore the default setting.	
	icmp-guard monitor-period <i>seconds</i>	
	no icmp-guard monitor-period	
	default icmp-guard monitor-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 seconds.
Defaults	The default is 600.	
Command	NFPP configuration mode	

Mode		
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.	
Configuration Examples	The following example sets the monitor time to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# icmp-guard monitor-period 180</pre>	
Related Commands	Command	Description
	show nfpp icmp-guard summary	Displays the configuration.
	show nfpp icmp-guard hosts	Displays the monitored host list.
	clear nfpp icmp-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.38 icmp-guard rate-limit

	Use this command to set the rate-limit threshold globally. Use the no or default form of this command to restore the default setting.	
	icmp-guard rate-limit { per-src-ip per-port } pps	
	no icmp-guard rate-limit { per-src-ip per-port }	
	default icmp-guard rate-limit { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the rate limit for each source IP address.
	per-port	Sets the rate limit for each port.
	<i>pps</i>	Sets the rate limit, in the range from 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	

Configuration	The following example sets the rate-limit threshold globally.	
Examples	FS(config)# nfpp FS(config-nfpp)# icmp-guard rate-limit per-src-ip 500 FS(config-nfpp)# icmp-guard rate-limit per-port 800	
Related Commands	Command	Description
	nfpp icmp-guard policy	Sets the rate limit and the attack threshold.
	show nfpp icmp-guard summary	Displays the configuration.
Platform Description	N/A	

21.39 icmp-guard trusted-host

	Use this command to set the trusted hosts free form monitoring. Use the no or default form of this command to restore the default setting.	
	icmp-guard trusted-host <i>ip mask</i>	
	no icmp-guard trusted-host { all <i>ip mask</i> }	
	default icmp-guard trusted-host	
Parameter Description	Parameter	Description
	<i>ip</i>	Sets the IP address.
	<i>mask</i>	Sets the IP mask.
	all	Deletes the configuration of all trusted hosts.
Defaults	No trusted host is configured by default.	
Command Mode	NFPP configuration mode	
Usage Guide	The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are allowed to send to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.	
Configuration Examples	The following example sets the trusted hosts free form monitoring. FS(config)# nfpp FS(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0	
Related Commands	Command	Description
	show nfpp icmp-guard trusted-host	Displays the configuration.

Platform	N/A
Description	

21.40 ip-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs. Use the no or default form of this command to restore the default setting.	
	ip-guard attack-threshold { per-src-ip per-port } pps	
	no ip-guard attack-threshold { per-src-ip per-port }	
	default ip-guard attack-threshold { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-port	Sets the attack threshold for each port.
	<i>pps</i>	Sets the attack threshold, in pps. The valid range is 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	The attack threshold shall be equal to or larger than the rate-limit threshold.	
Configuration Examples	The following example sets the global attack threshold. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard attack-threshold per-src-ip 2 FS(config-nfpp)# ip-guard attack-threshold per-port 50</pre>	
Related Commands	Command	Description
	nfpp ip-guard policy	Displays the rate-limit threshold and attack threshold.
	show nfpp ip-guard summary	Displays the configuration.
	show nfpp ip-guard hosts	Displays the monitored host list.
	clear nfpp ip-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.41 ip-guard enable

	Use this command to enable IP guard. Use the no or default form of this command to restore the default setting.	
	ip-guard enable	
	no ip-guard enable	
	default ip-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	NFPP configuration mode.	
Usage Guide	This configuration aims at attacks whose destination IP address is not the local one. For those with the local address as the destination, CPP (CPU Protect Policy) will limit their rates.	
Configuration Examples	The following example enables the IP guard globally. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard enable</pre>	
Related Commands	Command	Description
	nffp ip-guard enable	Enables the IP guard on the interface.
Platform Description	N/A	

21.42 ip-guard isolate-period

	Use this command to set the isolate time globally. Use the no or default form of this command to restore the default setting.	
	ip-guard isolate-period { seconds permanent }	
	no ip-guard isolate-period	
	default ip-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate time. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation

Defaults	The default isolate time is 0 second, which means no isolation.						
Command Mode	NFPP configuration mode						
Usage Guide	N/A.						
Configuration Examples	The following example sets the isolate time globally to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard isolate-period 180</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>nfpp ip-guard isolate-period</td><td>Sets the isolate time on the interface.</td></tr> <tr> <td>show nfpp ip-guard summary</td><td>Displays the configuration.</td></tr> </table>	Command	Description	nfpp ip-guard isolate-period	Sets the isolate time on the interface.	show nfpp ip-guard summary	Displays the configuration.
Command	Description						
nfpp ip-guard isolate-period	Sets the isolate time on the interface.						
show nfpp ip-guard summary	Displays the configuration.						
Platform Description	N/A						

21.43 ip-guard monitor-period

	Use this command to configure the monitor time. Use the no or default form of this command to restore the default setting.	
	ip-guard monitor-period <i>seconds</i>	
	no ip-guard monitor-period	
	default ip-guard monitor-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.
Defaults	The default is 600 seconds.	
Command Mode	NFPP configuration mode	
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software	

Configuration Examples	The following example sets the monitor time to 180 seconds. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard monitor-period 180</pre>	
Related Commands	Command	Description
	show nfpp ip-guard summary	Displays the configuration.
	show nfpp ip-guard hosts	Displays the monitored host list.
	clear nfpp ip-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.44 ip-guard monitored-host-limit

	Use this command to set the maximum monitored host number. Use the no or default form of this command to restore the default setting.	
	ip-guard monitored-host-limit <i>number</i>	
	no ip-guard monitored-host-limit	
	default ip-guard monitored-host-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20,000 seconds.	
Command Mode	NFPP configuration mode	
Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that % NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 20,000 monitored hosts to remind the administrator.	
Configuration Examples	The following example sets the maximum monitored host number to 200. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard monitored-host-limit 200</pre>	
Related Commands	Command	Description
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

21.45 ip-guard rate-limit

	Use this command to set the rate-limit threshold globally. Use the no or default form of this command to restore the default setting.	
	ip-guard rate-limit { per-src-ip per-port } <i>pps</i>	
	no ip-guard rate-limit { per-src-ip per-port }	
	default ip-guard rate-limit { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the rate limit for each source IP address.
	per-port	Sets the rate limit for each port.
	<i>pps</i>	Sets the rate limit, in the range of 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate-limit threshold globally. <pre> FS(config)# nfpp FS(config-nfpp)# ip-guard rate-limit per-src-ip 2 FS(config-nfpp)# ip-guard rate-limit per-port 50 </pre>	
Related Commands	Command	Description
	nfpp ip-guard policy	Sets the rate limit and the attack threshold.
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

21.46 ip-guard scan-threshold

	Use this command to set the global scan threshold. Use the no or default form of this command to restore the default setting.	
	ip-guard scan-threshold <i>pkt-cnt</i>	
	no ip-guard scan-threshold	
	default ip-guard scan-threshold	

Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode.	
Usage Guide	N/A	
Configuration Examples	The following example sets the global scan threshold to 20 pps. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard scan-threshold 20</pre>	
Related Commands	Command	Description
	nfpp ip-guard scan-threshold	Sets the scan threshold on the port.
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

21.47 ip-guard trusted-host

	Use this command to set the trusted hosts free form monitoring. Use the no or default form of this command to restore the default setting.	
	ip-guard trusted-host <i>ip mask</i>	
	no ip-guard trusted-host { all <i>ip mask</i> }	
	default ip-guard trusted-host	
Parameter Description	Parameter	Description
	<i>ip</i>	Sets the IP address.
	<i>mask</i>	Sets the IP mask.
	all	Deletes the configuration of all trusted hosts.
Defaults	N/A	
Command Mode	NFPP configuration mode	
Usage Guide	The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are	

	allowed to sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported.	
Configuration Examples	The following example sets the trusted hosts free form monitoring. <pre>FS(config)# nfpp FS(config-nfpp)# ip-guard trusted-host 1.1.1.0 255.255.255.0</pre>	
Related Commands	Command	Description
	show nfpp ip-guard trusted-host	Displays the configuration.
Platform Description	N/A	

21.48 log-buffer enable

	Use this command to display logs on the screen. Use the no or the default form of this command to restore the default setting.	
	log-buffer enable	
	no log-buffer enable	
	default log-buffer enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	Logs are stored in the cache by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example displays logs on the screen. <pre>FS(config)# nfpp FS(config-nfpp)# log-buffer enable</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

21.49 log-buffer entries

	Use this command to set the NFPP log buffer area size. Use the no or default form of this command to restore the default setting.	
	log-buffer entries <i>number</i>	
	no log-buffer entries	
	default log-buffer entries	
Parameter Description	Parameter	Description
	<i>number</i>	The buffer area size, in the range from 0 to 1,024.
Defaults	The default is 256.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the NFPP log buffer area size. <pre>FS(config)# nfpp FS(config-nfpp)# log-buffer entries 50</pre>	
Related Commands	Command	Description
	log-buffer logs <i>number_of_message interval length_in_seconds</i>	Displays the rate of the syslog generated from the NFPP buffer area.
	show nfpp log	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

21.50 log-buffer logs

	Use this command to set the rate of syslog generated from the NFPP log buffer area. Use the no or default form of this command to restore the default setting.	
	log-buffer logs <i>number_of_message interval length_in_seconds</i>	
	no log-buffer logs	
	default log-buffer logs	
Parameter Description	Parameter	Description
	<i>number_of_message</i>	The valid range is from 0 to 1024.

		0 indicates that all logs are recorded in the specific buffer area and no syslogs are generated.
	<i>length_in_seconds</i>	The valid range is from 0 to 86400(one day). 0 indicates not to write the log to the buffer area but generate the syslog immediately. With both the <i>number_of_message</i> and <i>length_in_seconds</i> values are 0, it indicates not to write the log to the buffer area but generate the syslog immediately. The parameter <i>number_of_message /length_in_second</i> indicates the rate of syslog generated from the NFPP log buffer area.
Defaults	By default, <i>number_of_message</i> is 0 and <i>length_in_seconds</i> is 0.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate of syslog generated from the NFPP log buffer area. <pre>FS(config)# nfpp FS(config-nfpp)# log-buffer logs 2 interval 12</pre>	
Related Commands	Command	Description
	log-buffer entries <i>number</i>	Sets the NFPP log buffer area size.
	show nfpp log summary	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

21.51 logging

	Use this command to set the VLAN or the interface log for NFPP. Use the no or default form of this command to restore the default setting.	
	logging vlan <i>vlan-range</i>	
	logging interface <i>interface-id</i>	
	no logging vlan <i>vlan-range</i>	
	no logging interface <i>interface-id</i>	
	default logging	
Parameter Description	Parameter	Description
	<i>vlan-range</i>	Sets the specified VLAN range, in the format such as "1-3, 5".

	<i>interface-id</i>	Sets the interface ID.
Defaults	All logs are recorded by default.	
Command Mode	NFPP configuration mode	
Usage Guide	Use this command to filter the logs and records the logs within the specified VLAN range or the specified port	
Configuration Examples	The following example records the logs in VLAN 1, VLAN 2, VLAN 3 and VLAN 5 only. <pre>FS(config)# nfpp FS(config-nfpp)# logging vlan 1-3,5</pre> The following example records the logs on the interface GigabitEthernet 0/1 only. <pre>FS(config)# nfpp FS(config-nfpp)# logging interface G 0/1</pre>	
Related Commands	Command	Description
	show nfpp log summary	Displays the NFPP log configuration or the log buffer area.
Platform Description	N/A	

21.52 match

	Use this command to specify the message matching filed for the user-defined anti-attack.	
	match [etype <i>type</i>] [src-mac <i>smac</i> [src-mac-mask <i>smac_mask</i>]] [dst-mac <i>dmac</i> [dst-mac-mask <i>dst_mask</i>]] [protocol <i>protocol</i>] [src-ip <i>sip</i> [src-ip-mask <i>sip-mask</i>]] [src-ipv6 <i>sip6</i> [src-ipv6-masklen <i>sip6-masklen</i>]] [dst-ip <i>dip</i> [dst-ip-mask <i>dip-mask</i>]] [dst-ipv6 <i>dip6</i> [dst-ipv6-masklen <i>dip6-masklen</i>]] [src-port <i>sport</i>] [dst-port <i>dport</i>]	
Parameter Description	Parameter	Description
	<i>type</i>	Ethernet link layer packet type
	<i>smac</i>	Source MAC address
	<i>smac_mask</i>	Source MAC address mask
	<i>dmac</i>	Destination MAC address
	<i>dmac_mask</i>	Destination MAC address mask
	<i>protocol</i>	IPv4/v6 message protocol
	<i>sip</i>	Source IPv4 address
	<i>sip_mask</i>	Source IPv4 address mask
	<i>sip6</i>	Source IPv6 address

	<i>sip6_masklen</i>	Source IPv6 address mask
	<i>dip</i>	Destination IPv4 address
	<i>dip_mask</i>	Destination IPv4 address mask
	<i>dip6</i>	Destination IPv6 address
	<i>dip6_masklen</i>	Length of the destination IPv6 address mask.
	<i>sport</i>	Source port
	<i>dport</i>	Destination port
Defaults	N/A	
Command Mode	NFPP configuration mode	
Usage Guide	Use this command to create a new user-defined anti-attack type and specify the message fields to be matched.	
Configuration Examples	The following example specifies the message matching filed for the user-defined anti-attack. <pre>FS(config)# nfpp FS(config-nfpp)# nfpp define tcp FS(config-nfpp-define)#match etype 0x0800 protocol 0x06</pre>	
Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration
Platform Description	N/A	

21.53 monitored-host-limit

	Use this command to set the maximum monitored host number. Use the no or default form of this command to restore the default setting.	
	monitored-host-limit <i>number</i>	
	no monitored-host-limit	
	default monitored-host-limit	
Parameter Description	Parameter	Description
	<i>number</i>	The maximum monitored host number, in the range from 1 to 4,294,967,295.
Defaults	The default is 20,000.	
Command Mode	NFPP define configuration mode	

Usage Guide	If the monitored host number has reached the default 20,000, the administrator shall set the max-number smaller than 20,000 and it will prompt the message that %ERROR: The value that you configured is smaller than current monitored hosts 20,000, please clear a part of monitored hosts to remind the administrator of the invalid configuration and removing the monitored hosts. When the maximum monitored host number has been exceeded, it prompts the message that % % NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name's 20,000 monitored hosts. to remind the administrator	
Configuration Examples	The following example sets the maximum monitored host number. <pre>FS(config)# nfpp FS(config-nfpp)# nfpp define tcp FS(config-nfpp-define)#monitored-host-limit 500</pre>	
Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration
Platform Description	N/A	

21.54 monitor period

	Use this command to set the monitoring time. Use the no or default form of this command to restore the default setting.	
	monitor-period <i>seconds</i>	
	no monitor-period	
	default monitor-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the monitor time, in the range from 180 to 86,400 in the unit of seconds.
Defaults	The default is 600 seconds.	
Command Mode	NFPP define configuration mode	
Usage Guide	When the attacker is detected, if the isolate period is 0, the attacker will be monitored by the software and the timeout time will be the monitor period. During the software monitoring, if the isolate period is not 0, the software-monitored attacker will be auto-isolated by the hardware and the timeout time will be the isolate period. The monitor period is valid with the isolate period 0. If the isolate period has changed to be 0, the attackers on the interface will be removed rather than being monitored by the software.	

Configuration	The following example sets the monitoring time to 1,000 seconds.	
Examples	FS(config)# nfpp FS(config-nfpp)# define tcp FS(config-nfpp-define)#monitor-period 1000	
Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration.
Platform Description	N/A	

21.55 nd-guard attack-threshold

	Use this command to set the global attack threshold. When the packet rate exceeds the attack threshold, the attack occurs.	
	Use the no or default form of this command to restore the default setting.	
	nd-guard attack-threshold per-port { ns-na rs ra-redirect } pps	
	no nd-guard attack-threshold per-port { ns-na rs ra-redirect }	
	default nd-guard attack-threshold per-port { ns-na rs ra-redirect }	
Parameter Description	Parameter	Description
	ns-na	Sets the neighbor request and neighbor advertisement.
	rs	Sets the router request.
	ra-redirect	Sets the router advertisement and the redirect packets.
	pps	Sets the attack threshold, in the range from 1 to 19999 in the unit of seconds.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode.	
Usage Guide	The attack threshold shall be equal to or larger than the rate-limit threshold.	
Configuration Examples	The following example sets the global attack threshold. FS(config)# nfpp FS(config-nfpp)# nd-guard attack-threshold per-port ns-na 20 FS(config-nfpp)# nd-guard attack-threshold per-port rs 10 FS(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10	
Related Commands	Command	Description
	nfpp ip-guard policy	Displays the rate-limit threshold and attack

		threshold.
	show nfpp ip-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.56 nd-guard enable

	Use this command to enable the ND anti-attack function. Use the no or default form of this command to restore the default setting.	
	nd-guard enable	
	no nd-guard enable	
	default nd-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is enabled by default.	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the ND anti-attack function. <pre>FS(config)# nfpp FS(config-nfpp)# nd-guard enable</pre>	
Related Commands	Command	Description
	nfpp nd-guard enable	Enables the ND anti-attack function on the interface.
	show nfpp nd-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.57 nd-guard rate-limit

	Use this command to set the rate-limit threshold globally. Use the no or default form of this command to restore the default setting.	
	nd-guard rate-limit per-port { ns-na rs ra-redirect } pps	
	no nd-guard rate-limit per-port { ns-na rs ra-redirect }	
	default nd-guard rate-limit per-port { ns-na rs ra-redirect }	

Parameter Description	Parameter	Description
	ns-na	Sets the neighbor request and neighbor advertisement.
	rs	Sets the router request.
	ra-redirect	Sets the router advertisement and the redirect packets.
	<i>pps</i>	Sets the attack threshold, in the range is from 1 to 19,999 in the unit of pps.
Defaults	The default value varies with products. For details, see the <i>Configuration Guide</i> .	
Command Mode	NFPP configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the rate-limit threshold globally. <pre> FS(config)# nfpp FS(config-nfpp)# nd-guard rate-limit per-port ns-na 10 FS(config-nfpp)# nd-guard rate-limit per-port rs 5 FS(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5 </pre>	
Related Commands	Command	Description
	nfpp nd-guard policy	Sets the rate limit and the attack threshold.
	show nfpp nd-guard summary	Displays the configuration.
Platform Description	N/A	

21.58 nd-guard ratelimit-forwarding enable

	Use this command to enable the ND-guard ratelimit-forwarding on the interface.	
	nd-guard ratelimit-forwarding enable	
	Use this command to disable the ND-guard ratelimit-forwarding on the interface.	
	no nd-guard ratelimit-forwarding enable	
	Use this command to restore the default setting.	
	default nd-guard ratelimit-forwarding enable	
Parameter Description	Parameter	Description
	N/A	N/A

Defaults	The function is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A
Configuration Examples	The following example enables the ND-guard ratelimit-forwarding on the interface. <pre>FS(config)# nfpp FS(config-nfpp)# nd-guard ratelimit-forwarding enable</pre>
Platform Description	N/A

21.59 nfpp

	Use this command to enter NFPP configuration mode. nfpp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Global configuration mode	
Usage Guide	Use this command to enter NFPP configuration mode and make further configuration.	
Configuration Examples	The following example enters NFPP configuration mode. <pre>FS(config)# nfpp</pre>	
Platform Description	N/A	

21.60 nfpp arp-guard enable

	Use this command to enable the anti-ARP attack function on the interface. Use the no or default form of this command to restore the default setting.
	nfpp arp-guard enable
	no nfpp arp-guard enable
	default nfpp arp-guard enable

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The anti-ARP attack function is not enabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	The interface anti-ARP attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the anti-ARP attack function on the interface. <pre>FS(config)# interface G0/1 FS(config-if)# nfpp arp-guard enable</pre>	
Related Commands	Command	Description
	arp-guard enable	Enables the anti-ARP attack function.
	show nfpp arp-guard summary	Displays the configuration.
Platform Description	N/A	

21.61 nfpp arp-guard isolate-period

	Use this command to set the isolate period in the interface configuration mode. Use the no or default form of this command to restore the default setting.	
	nfpp arp-guard isolate-period { <i>seconds</i> permanent }	
	no nfpp arp-guard isolate-period	
	default nfpp arp-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate period. The value is 0, or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation
Defaults	By default, the isolate period is not configured.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	

Configuration	The following example sets the isolate period in the interface configuration mode.	
Examples	FS(config)# interface G0/1 FS(config-if)# nfpp arp-guard isolate-period 180	
Related Commands	Command	Description
	arp-guard isolate-period	Sets the global isolate period.
	show nfpp arp-guard summary	Displays the configuration.
Platform Description	N/A	

21.62 nfpp arp-guard policy

	Use this command to set the rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.	
	nfpp arp-guard policy { per-src-ip per-src-mac per-port } rate-limit-pps attack-threshold-pps	
	no nfpp arp-guard policy { per-src-ip per-src-mac per-port }	
	default nfpp arp-guard policy { per-src-ip per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from1 to 19999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold. FS(config)# interface G 0/1 FS(config-if)# nfpp arp-guard policy per-src-ip 2 10 FS(config-if)# nfpp arp-guard policy per-src-mac 3 10 FS(config-if)# nfpp arp-guard policy per-port 50 100	

Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	arp-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard hosts	Displays the monitored host.
	clear nfpp arp-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.63 nfpp arp-guard scan-threshold

	Use this command to set the scan threshold. Use the no or default form of this command to restore the default setting.	
	nfpp arp-guard scan-threshold <i>pkt-cnt</i>	
	no nfpp arp-guard scan-threshold	
	default nfpp arp-guard scan-threshold	
Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.
Defaults	By default, the sport-based scan threshold is not configured.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the scan threshold to 20 pps. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp arp-guard scan-threshold 20</pre>	
Related Commands	Command	Description
	arp-guard attack-threshold	Sets the global attack threshold.
	show nfpp arp-guard summary	Displays the configuration.
	show nfpp arp-guard scan	Displays the ARP scan table.
	clear nfpp arp-guard scan	Clears the ARP scan table.
Platform Description	N/A	

21.64 nfpp define name enable

	Use this command to enable the user-defined anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp define name enable	
	no nfpp define name enable	
	default nfpp define name enable	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type
Defaults	N/A	
Command Mode	Interface configuration mode.	
Usage Guide	This command takes effect only after the name of the user-defined anti-attack and the match, rate-count, rate-limit and the attack-threshold have been configured.	
Configuration Examples	The following example enables the user-defined anti-attack function on the interface. <pre>FS(config)# interface G0/1 FS(config-if)# nfpp define tcp enable</pre>	
Related Commands	Command	Description
	show nfpp define summary	Displays the user-defined anti-attack configuration.
Platform Description	N/A	

21.65 nfpp define policy

	Use this command to set the local rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.	
	nfpp define name policy { per-src-ip per-src-mac per-port } rate-limit-pps attack-threshold-pps	
	no nfpp define name policy { per-src-ip per-src-mac per-port }	
	default nfpp define name policy { per-src-ip per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the attack threshold for each source IP address.
	per-src-mac	Sets the attack threshold for each source MAC address.
	per-port	Sets the attack threshold for each port.

	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range of from 1 to 19,999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the local rate-limit threshold and the attack threshold. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp define tcp policy per-src-ip 2 10 FS(config-if)# nfpp define tcp policy per-port 50 100</pre>	
Related Commands	Command	Description
	define-policy	Sets the global rate-limit threshold and attack threshold.
	show nfpp define summary	Displays the user-defined anti-attack configuration.
Platform Description	N/A	

21.66 nfpp dhcp-guard enable

	Use this command to enable the DHCP anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp dhcp-guard enable	
	no nfpp dhcp-guard enable	
	default nfpp dhcp-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The DHCP anti-attack function is not enabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	The interface DHCP anti- attack configuration is prior to the global configuratio	
Configuration	The following example enables the DHCP anti-attack function on the interface.	

Examples	FS(config)# interface G0/1	
	FS(config-if)# nfpp dhcp-guard enable	
Related Commands	Command	Description
	dhcp-guard enable	Enables the anti-ARP attack function.
	show nfpp dhcp-guard summary	Displays the configuration.
Platform Description	N/A	

21.67 nfpp dhcp-guard policy

	Use this command to set the rate-limit threshold and the attack threshold on the port. Use the no or default form of this command to restore the default setting.	
	nfpp dhcp-guard policy { per-src-mac per-port } rate-limit-pps attack-threshold-pps	
	no nfpp dhcp-guard policy { per-src-mac per-port }	
	default nfpp dhcp-guard policy { per-src-mac per-port }	
Parameter Description	Parameter	Description
	per-src-mac	Sets the rate-limit threshold and the attack threshold for the designated source MAC address.
	per-port	Sets the rate-limit threshold and the attack threshold for the designated port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.
Defaults	The rate-limit threshold and the attack threshold are not configured by default. So the device adopts the rate-limit threshold and the attack threshold that are set in the global configuration mode.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold on interface G0/1.	
	FS(config)#interface G 0/1 FS(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10 FS(config-if)# nfpp dhcpv6-guard policy per-port 50 100	
Related Commands	Command	Description
	N/A	N/A

Platform	N/A
Description	

21.68 nfpp dhcpv6-guard enable

	Use this command to enable the DHCPv6 anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp dhcpv6-guard enable	
	no nfpp dhcpv6-guard enable	
	default nfpp dhcpv6-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The DHCPv6 anti-attack function is not enabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	The interface DHCPv6 anti- attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the DHCPv6 anti-attack function on interface G0/1. FS(config)# interface G0/1 FS(config-if)# nfpp dhcpv6-guard enable	
Related Commands	Command	Description
	dhcpv6-guard enable	Enables the anti-ARP attack function.
	show nfpp dhcpv6-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.69 nfpp dhcpv6-guard policy

	Use this command to set the rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.
	nfpp dhcpv6-guard policy { per-src-mac per-port } rate-limit-pps attack-threshold-pps
	no nfpp dhcpv6-guard policy { per-src-mac per-port }
	default nfpp dhcpv6-guard policy { per-src-mac per-port }

Parameter Description	Parameter	Description
	per-src-mac	Sets the rate-limit threshold and the attack threshold for each source MAC address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range of from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10 FS(config-if)# nfpp dhcpv6-guard policy per-port 50 100</pre>	
Related Commands	Command	Description
	dhcpv6-guard attack-threshold	Sets the global attack threshold.
	dhcpv6-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp dhcpv6-guard summary	Displays the configuration.
	show nfpp dhcpv6-guard hosts	Displays the monitored host.
	clear nfpp dhcpv6-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.70 nfpp icmp-guard enable

	Use this command to enable the ICMP anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp icmp-guard enable	
	no nfpp icmp-guard enable	
	default nfpp icmp-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The ICMP anti-attack function is not enabled on the interface.	

Command Mode	Interface configuration mode	
Usage Guide	The interface ICMP anti- attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the ICMP anti-attack function on the interface. FS(config)# interface G0/1 FS(config-if)# nfpp icmp-guard enable	
Related Commands	Command	Description
	icmp-guard enable	Enables the anti-ARP attack function.
	show nfpp icmp-guard summary	Displays the configuration.
Platform Description	N/A	

21.71 nfpp icmp-guard isolate-period

	Use this command to set the isolate period in the interface configuration mode. Use the no or default form of this command to restore the default setting.	
	nfpp icmp-guard isolate-period { <i>seconds</i> permanent }	
	no nfpp icmp-guard isolate-period	
	default nfpp icmp-guard isolate-period	
Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate period. The value is 0 or in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation
Defaults	By default, the isolate period is not configured.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the isolate period in the interface configuration mode. FS(config)# interface G0/1 FS(config-if)# nfpp icmp-guard isolate-period 180	

Related Commands	Command	Description
	icmp-guard isolate-period	Sets the global isolate period.
	show nfpp icmp-guard summary	Displays the configuration.
Platform Description	N/A	

21.72 nfpp icmp-guard policy

	Use this command to set the rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.	
	nfpp icmp-guard policy { per-src-ip per-port } rate-limit-pps attack-threshold-pps	
	no nfpp icmp-guard policy { per-src-ip per-port }	
	default nfpp icmp-guard policy { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in range from 1 to 19,999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp icmp-guard policy per-src-ip 5 10 FS(config-if)# nfpp icmp-guard policy per-port 100 200</pre>	
Related Commands	Command	Description
	icmp-guard attack-threshold	Sets the global attack threshold.
	icmp-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp icmp-guard summary	Displays the configuration.
	show nfpp icmp-guard hosts	Displays the monitored host.
	clear nfpp icmp-guard hosts	Clears the isolated host.

Platform	N/A
Description	

21.73 nfpp ip-guard enable

	Use this command to enable the IP anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp ip-guard enable	
	no nfpp ip-guard enable	
	default nfpp ip-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The IP anti-attack function is disabled on the interface.	
Command Mode	Interface configuration mode	
Usage Guide	The interface IP anti-attack configuration is prior to the global configuration.	
Configuration Examples	The following example enables the IP anti-attack function on the interface. <pre>FS(config)# interface G0/1 FS(config-if)# nfpp ip-guard enable</pre>	
Related Commands	Command	Description
	ip-guard enable	Enables the anti-ARP attack function.
	show nfpp ip-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.74 nfpp ip-guard isolate-period

	Use this command to set the isolate period in the interface configuration mode. Use the no or default form of this command to restore the default setting.	
	nfpp ip-guard isolate-period { seconds permanent }	
	no nfpp ip-guard isolate-period	
	default nfpp ip-guard isolate-period	

Parameter Description	Parameter	Description
	<i>seconds</i>	Sets the isolate period, in the range from 30 to 86,400 in the unit of seconds.
	permanent	Permanent isolation
Defaults	By default, the isolate period is not configured.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the isolate period in the interface configuration mode. <pre>FS(config)# interface G0/1 FS(config-if)# nfpp ip-guard isolate-period 180</pre>	
Related Commands	Command	Description
	ip-guard isolate-period	Sets the global isolate period.
	show nfpp ip-guard summary	Displays the configuration.
Platform Description	N/A	

21.75 nfpp ip-guard policy

	Use this command to set the rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.	
	nfpp ip-guard policy { per-src-ip per-port } rate-limit-pps attack-threshold-pps	
	no nfpp ip-guard policy { per-src-ip per-port }	
	default nfpp ip-guard policy { per-src-ip per-port }	
Parameter Description	Parameter	Description
	per-src-ip	Sets the rate-limit threshold and the attack threshold for each source IP address.
	per-port	Sets the rate-limit threshold and the attack threshold for each port.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	

Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp ip-guard policy per-src-ip 2 10 FS(config-if)# nfpp ip-guard policy per-port 50 100</pre>	
Related Commands	Command	Description
	ip-guard attack-threshold	Sets the global attack threshold.
	ip-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp ip-guard summary	Displays the configuration.
	show nfpp ip-guard hosts	Displays the monitored host.
	clear nfpp ip-guard hosts	Clears the isolated host.
Platform Description	N/A	

21.76 nfpp ip-guard scan-threshold

	Use this command to set the scan threshold. Use the no or default form of this command to restore the default setting.	
	nfpp ip-guard scan-threshold <i>pkt-cnt</i>	
	no nfpp ip-guard scan-threshold	
	default nfpp ip-guard scan-threshold	
Parameter Description	Parameter	Description
	<i>pkt-cnt</i>	Sets the scan threshold, in the range from 1 to 19,999.
Defaults	By default, the sport-based scan threshold is not configured.	
Command Mode	Interface configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example sets the scan threshold to 20pps. <pre>FS(config)# interface G 0/1 FS(config-if)# nfpp ip-guard scan-threshold 20</pre>	
Related Commands	Command	Description

	ip-guard attack-threshold	Sets the global attack threshold.
	show nfpp ip-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.77 nfpp nd-guard enable

	Use this command to enable the ND anti-attack function on the interface. Use the no or default form of this command to restore the default setting.	
	nfpp nd-guard enable	
	no nfpp nd-guard enable	
	default nfpp nd-guard enable	
Parameter		
Description	Parameter	Description
	N/A	N/A
Defaults	The ND anti-attack function is disabled on the interface.	
Command	Interface configuration mode	
Mode		
Usage Guide	The interface ND anti-attack configuration is prior to the global configuration.	
Configuration	The following example enables the ND anti-attack function on the interface.	
Examples	<pre>FS(config)# interface G0/1 FS(config-if)# nfpp nd-guard enable</pre>	
Related		
Commands	Command	Description
	nd-guard enable	Enables the ND anti-attack function.
	show nfpp nd-guard summary	Displays the configuration.
Platform	N/A	
Description		

21.78 nfpp nd-guard policy

	Use this command to set the rate-limit threshold and the attack threshold. Use the no or default form of this command to restore the default setting.
	nfpp nd-guard policy per-port { ns-na rs ra-redirect } rate-limit-pps attack-threshold-pps
	no nfpp nd-guard policy per-port { ns-na rs ra-redirect }
	default nfpp nd-guard policy per-port { ns-na rs ra-redirect }

Parameter Description	Parameter	Description
	ns-na	Sets the neighbor request and neighbor advertisement.
	rs	Sets the router request.
	ra-redirect	Sets the router advertisement and the redirect packets.
	<i>rate-limit-pps</i>	Sets the rate-limit threshold, in the range from 1 to 19,999.
	<i>attack-threshold-pps</i>	Sets the attack threshold, in the range from 1 to 19,999.
Defaults	By default, the rate-limit threshold and the attack threshold are not configured.	
Command Mode	Interface configuration mode	
Usage Guide	The attack threshold value shall be equal to or greater than the rate-limit threshold.	
Configuration Examples	The following example sets the rate-limit threshold and the attack threshold. <pre> FS(config)# interface G 0/1 FS(config-if)# nfpp nd-guard policy per-port ns-na 50 100 FS(config-if)# nfpp nd-guard policy per-port rs 10 20 FS(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20 </pre>	
Related Commands	Command	Description
	nd-guard attack-threshold	Sets the global attack threshold.
	nd-guard rate-limit	Sets the global rate-limit threshold.
	show nfpp nd-guard summary	Displays the configuration.
Platform Description	N/A	

21.79 show nfpp arp-guard hosts

	Use this command to display the monitored host.	
	show nfpp arp-guard hosts [statistics] [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i> <i>mac-address</i>]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the monitored host.
	<i>vid</i>	The VLAN ID
	<i>interface-id</i>	The interface name
	<i>ip-address</i>	The IP address
	<i>mac-address</i>	The MAC address

Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	N/A				
Configuration Examples	The following example displays the statistical information of the monitored host. <pre>FS# show nfpp arp-guard hosts statistics success fail total ----- 100 20 120</pre> The following example shows the monitored host. <pre>FS# show nfpp arp-guard hosts If column 1 shows '*', it means "hardware do not isolate user". VLAN interface IP address MAC address remain-time(s) ----- 1 Gi0/1 1.1.1.1 - 110 2 Gi0/2 1.1.2.1 - 61 *3 Gi0/3 - 0000.0000.1111 110 4 Gi0/4 - 0000.0000.2222 61 Total:4 hosts</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>clear nfpp arp-guard hosts</td><td>Clears the monitored hosts.</td></tr> </table>	Command	Description	clear nfpp arp-guard hosts	Clears the monitored hosts.
Command	Description				
clear nfpp arp-guard hosts	Clears the monitored hosts.				
Platform Description	N/A				

21.80 show nfpp arp-guard scan

	Use this command to display the ARP scan list.	
	show nfpp arp-guard scan [statistics] [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>] [<i>mac-address</i>]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the ARP scan list.
	<i>vid</i>	The VLAN ID
	<i>interface-id</i>	The interface name
	<i>ip-address</i>	The IP address
	<i>mac-address</i>	The MAC address

Defaults	N/A				
Command Mode	Privileged EXEC mode				
Usage Guide	N/A				
Configuration Examples	The following example displays the ARP scan list.				
	FS# show nfpp arp-guard scan statistics				
	arp-guard table has 4 record(s).				
	The following example displays the ARP scan list.				
	FS# show nfpp arp-guard scan				
	VLAN	interface	IP address	MAC address	timestamp
	----	-----	-----	-----	
	1	Gi0/1	-	0000.0000.0001	2008-01-23 16:23:10
	2	Gi0/2	1.1.1.1	0000.0000.0002	2008-01-23 16:24:10
	3	Gi0/3	-	0000.0000.0003	2008-01-23 16:25:10
	4	Gi0/4	-	0000.0000.0004	2008-01-23 16:26:10
	Total:4 record(s)				
	The following example displays the ARP scan list.				
	FS# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001				
	VLAN	interface	IP address	MAC address	timestamp
	----	-----	-----	-----	
	1	Gi0/1	-	0000.0000.0001	2008-01-23 16:23:10
	Total:1 record(s)				
Related Commands	Command		Description		
	arp-guard scan-threshold		Sets the global scan threshold.		
	nfpp arp-guard scan-threshold		Sets the scan threshold.		
	clear nfpp arp-guard scan		Clears the ARP scan list.		
Platform Description	N/A				

21.81 show nfpp arp-guard summary

	Use this command to display the configuration.
	show nfpp arp-guard summary

Parameter Description	Parameter	Description																																				
	N/A	N/A																																				
Defaults	N/A																																					
Command Mode	Privileged EXEC mode																																					
Usage Guide	N/A																																					
Configuration Examples	The following example displays the configuration. FS# show nfpp arp-guard summary (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) <table><tr><td>Interface</td><td>Status</td><td>Isolate-period</td><td>Rate-limit</td><td>Attack-threshold</td><td>Scan-threshold</td></tr><tr><td>Global</td><td>Enable</td><td>300</td><td>4/5/60</td><td>8/10/100</td><td>15</td></tr><tr><td>Gi 0/1</td><td>Enable</td><td>180</td><td>5/-/-</td><td>8/-/-</td><td>-</td></tr><tr><td>Gi 0/2</td><td>Disable</td><td>200</td><td>4/5/60</td><td>8/10/100</td><td>20</td></tr></table> Maximum count of monitored hosts: 1000 Monitor period:300s <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface(Global)</td><td>Global configuration</td></tr><tr><td>Status</td><td>Enables/Disables the anti-attack function.</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr><tr><td>Scan-threshold</td><td>Scan threshold</td></tr></table>		Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Scan-threshold	Global	Enable	300	4/5/60	8/10/100	15	Gi 0/1	Enable	180	5/-/-	8/-/-	-	Gi 0/2	Disable	200	4/5/60	8/10/100	20	Field	Description	Interface(Global)	Global configuration	Status	Enables/Disables the anti-attack function.	Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port	Attack-threshold	In the same format as the rate-limit.	Scan-threshold	Scan threshold
Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Scan-threshold																																	
Global	Enable	300	4/5/60	8/10/100	15																																	
Gi 0/1	Enable	180	5/-/-	8/-/-	-																																	
Gi 0/2	Disable	200	4/5/60	8/10/100	20																																	
Field	Description																																					
Interface(Global)	Global configuration																																					
Status	Enables/Disables the anti-attack function.																																					
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port																																					
Attack-threshold	In the same format as the rate-limit.																																					
Scan-threshold	Scan threshold																																					
Related Commands	Command	Description																																				
	arp-guard attack-threshold	Sets the global attack threshold.																																				
	arp-guard enable	Enables the anti-ARP attack function.																																				
	arp-guard isolate-period	Sets the global isolate time.																																				
	arp-guard monitor-period	Sets the monitor period.																																				
	arp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.																																				
	arp-guard rate-limit	Sets the global rate-limit threshold.																																				
	arp-guard scan-threshold	Sets the global scan threshold.																																				
	nfpp arp-guard enable	Enables the anti-ARP attack function on the interface.																																				
	nfpp arp-guard isolate-period	Sets the isolate time.																																				
	nfpp arp-guard policy	Sets the rate-limit threshold and attack threshold.																																				

	nfpp arp-guard scan-threshold	Sets the scan threshold.
Platform	N/A	
Description		

21.82 show nfpp define hosts

	Use this command to display the monitored hosts.	
	show nfpp define hosts <i>name</i> [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>] [<i>mac-address</i>] [<i>ipv6-address</i>]]]	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type
	statistics	Displays the statistics of monitored hosts.
	<i>vid</i>	VLAN ID
	<i>interface-id</i>	Interface name
	<i>ip-address</i>	IP address
	<i>mac-address</i>	MAC address
	<i>ipv6-address</i>	IPv6 address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	This command allows filtering the hosts with parameters specified	
Configuration Examples	The following example displays the monitored hosts. FS#show nfpp define hosts abc If col_filter 1 shows '*', it means "hardware do not isolate host". VLAN interface MAC address remain-time(s) ----- *1 Gi4/2 00d0.f822.33e5 592 Total: 1 host	
Related Commands	Command	Description
	clear nfpp define hosts	Clears the monitored hosts of user-defined anti-attack type.
Platform Description	N/A	

21.83 show nfpp define summary

	Use this command to display the configuration.																							
	show nfpp define summary [<i>name</i>]																							
Parameter Description	Parameter	Description																						
	<i>name</i>	Name of the user-defined anti-attack type																						
Defaults	N/A																							
Command Mode	Privileged EXEC mode																							
Usage Guide	This command can be used to display the configuration. Without the name specified, all user-defined anti-attack types will be displayed.																							
Configuration Examples	The following example displays the configuration. <pre>FS#show nfpp define summary abc</pre> Define abc summary: <pre>match etype 0x800 src-ip 1.1.1.1 src-ip-mask 255.255.255.255</pre> Maximum count of monitored hosts: 20000 Monitor period:600s (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) <table><tr><td>Interface</td><td>Status</td><td>Rate-limit</td><td>Attack-threshold</td></tr><tr><td>Global</td><td>Disable</td><td>-/10/-</td><td>-/20/-</td></tr><tr><td>Gi4/1</td><td>Enable</td><td>-/-/-</td><td>-/-/-</td></tr></table> <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface</td><td>If the interface field is displayed as Global, it means that is configured in the global configuration mode.</td></tr><tr><td>Status</td><td>Enables/ Disables the anti-attack function.</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr></table>		Interface	Status	Rate-limit	Attack-threshold	Global	Disable	-/10/-	-/20/-	Gi4/1	Enable	-/-/-	-/-/-	Field	Description	Interface	If the interface field is displayed as Global, it means that is configured in the global configuration mode.	Status	Enables/ Disables the anti-attack function.	Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port	Attack-threshold	In the same format as the rate-limit.
Interface	Status	Rate-limit	Attack-threshold																					
Global	Disable	-/10/-	-/20/-																					
Gi4/1	Enable	-/-/-	-/-/-																					
Field	Description																							
Interface	If the interface field is displayed as Global, it means that is configured in the global configuration mode.																							
Status	Enables/ Disables the anti-attack function.																							
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port																							
Attack-threshold	In the same format as the rate-limit.																							
Related Commands	Command	Description																						
	match	Clears the monitored hosts of user-defined anti-attack type.																						
	policy	Attack threshold and rate-limit threshold.																						
	isolate-period	Isolates time																						
	monitored-period	Monitored time																						
	monitored-host-limit	Maximum monitored host number																						

Platform	N/A
Description	

21.84 show nfpp define trusted-host

	Use this command to display the trusted host free from monitoring.	
	show nfpp define trusted-host <i>name</i>	
Parameter Description	Parameter	Description
	<i>name</i>	Name of the user-defined anti-attack type
Defaults	N/A.	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the trusted host configuration. <pre>FS# show nfpp define trusted-host tcp Define tcp: IP address mask ----- 1.1.1.0 255.255.255.0 1.1.2.0 255.255.255.0 Total:2 record(s)</pre>	
Related Commands	Command	Description
	trusted-host	Configures the trusted hosts.
Platform	N/A	
Description		

21.85 show nfpp dhcp-guard hosts

	Use this command to display the monitored host.	
	show nfpp dhcp-guard hosts [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>mac-address</i>]]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the monitored host.
	<i>vid</i>	VLAN ID

	<i>interface-id</i>	Interface name
	<i>mac</i>	MAC address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the monitored host.	
	<pre>FS# show nfpp dhcp-guard hosts statistics success fail total ----- 100 20 120</pre>	
	The following example displays the monitored host.	
	<pre>FS# show nfpp dhcp-guard hosts If column 1 shows '*', it means "hardware failed to isolate host". VLAN interface MAC address remain-time(seconds) --- ----- - 1 gi0/2 0000.0000.0001 10 *2 gi0/1 0000.0000.0002 20 Total:2 host(s)</pre>	
Related Commands	Command	Description
	clear nfpp dhcp-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.86 show nfpp dhcp-guard summary

	Use this command to display the configuration.	
	show nfpp dhcp-guard summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode	

Mode																																			
Usage Guide	N/A																																		
Configuration Examples	The following example displays the configuration. <pre>FS# show nfpp dhcp-guard summary</pre> (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) <table><tr><td>Interface</td><td>Status</td><td>Isolate-period</td><td>Rate-limit</td><td>Attack-threshold</td></tr><tr><td>Global</td><td>Enable</td><td>300</td><td>-/5/150</td><td>-/10/300</td></tr><tr><td>Gi 0/1</td><td>Enable</td><td>180</td><td>-/6/-</td><td>-/8/-</td></tr><tr><td>Gi 0/2</td><td>Disable</td><td>200</td><td>-/5/30</td><td>-/10/50</td></tr></table> Maximum count of monitored hosts: 1000 Monitor period:300s <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface(Global)</td><td>Global configuration</td></tr><tr><td>Status</td><td>Enables/Disables the anti-attack function.</td></tr><tr><td>Isolate-period</td><td>Isolate period</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr></table>			Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Global	Enable	300	-/5/150	-/10/300	Gi 0/1	Enable	180	-/6/-	-/8/-	Gi 0/2	Disable	200	-/5/30	-/10/50	Field	Description	Interface(Global)	Global configuration	Status	Enables/Disables the anti-attack function.	Isolate-period	Isolate period	Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port	Attack-threshold	In the same format as the rate-limit.
Interface	Status	Isolate-period	Rate-limit	Attack-threshold																															
Global	Enable	300	-/5/150	-/10/300																															
Gi 0/1	Enable	180	-/6/-	-/8/-																															
Gi 0/2	Disable	200	-/5/30	-/10/50																															
Field	Description																																		
Interface(Global)	Global configuration																																		
Status	Enables/Disables the anti-attack function.																																		
Isolate-period	Isolate period																																		
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port																																		
Attack-threshold	In the same format as the rate-limit.																																		
Related Commands	Command	Description																																	
	dhcp-guard attack-threshold	Sets the global attack threshold.																																	
	dhcp-guard enable	Enables the DHCP anti-attack function.																																	
	dhcp-guard isolate-period	Sets the global isolate time.																																	
	dhcp-guard monitor-period	Sets the monitor period.																																	
	dhcp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.																																	
	dhcp-guard rate-limit	Sets the global rate-limit threshold.																																	
	nfpp dhcp-guard enable	Enables the DHCP anti-attack function on the interface.																																	
	nfpp dhcp-guard isolate-period	Sets the isolate time.																																	
	nfpp dhcp-guard policy	Sets the rate-limit threshold and attack threshold.																																	
Platform Description	N/A																																		

21.87 show nfpp dhcpv6-guard hosts

	Use this command to display the monitored host.
	show nfpp dhcpv6-guard hosts [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>mac-address</i>]]]

Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the monitored host.
	<i>vid</i>	The VLAN ID
	<i>interface-id</i>	The interface name
	<i>mac-address</i>	The MAC address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the monitored host. <pre> FS# show nfpp dhcpv6-guard hosts If column 1 shows '*', it means "hardware failed to isolate host". VLAN interface MAC address remain-time(seconds) ----- *1 gi0/2 0000.0000.0001 10 *2 gi0/1 0000.0000.0002 20 Total:2 host(s) </pre>	
Related Commands	Command	Description
	clear nfpp dhcpv6-guard hosts	Clears the monitored host.
Platform Description	N/A	

21.88 show nfpp dhcpv6-guard summary

	Use this command to display the configuration.	
	show nfpp dhcpv6-guard summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A																			
Configuration Examples	The following example displays the configuration. <pre>FS#show nfpp dhcpv6-guard summary</pre> (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) <table><tr><td>Interface</td><td>Status</td><td>Rate-limit</td><td>Attack-threshold</td></tr><tr><td>Global</td><td>Enable</td><td>-/5/1200</td><td>-/10/1500</td></tr></table> Maximum count of monitored hosts: 20000 Monitor period: 600s <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface(Global)</td><td>Global configuration</td></tr><tr><td>Status</td><td>Enables/Disables the anti-attack function.</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr></table>		Interface	Status	Rate-limit	Attack-threshold	Global	Enable	-/5/1200	-/10/1500	Field	Description	Interface(Global)	Global configuration	Status	Enables/Disables the anti-attack function.	Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port	Attack-threshold	In the same format as the rate-limit.
Interface	Status	Rate-limit	Attack-threshold																	
Global	Enable	-/5/1200	-/10/1500																	
Field	Description																			
Interface(Global)	Global configuration																			
Status	Enables/Disables the anti-attack function.																			
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port																			
Attack-threshold	In the same format as the rate-limit.																			
Related Commands	Command	Description																		
	dhcpv6-guard attack-threshold	Sets the global attack threshold.																		
	dhcpv6-guard enable	Enables the DHCPv6 anti-attack function.																		
	dhcpv6-guard monitor-period	Sets the monitor period.																		
	dhcpv6-guard monitored-host-limit	Sets the maximum number of the monitored hosts.																		
	dhcpv6-guard rate-limit	Sets the global rate-limit threshold.																		
	nfpp dhcpv6-guard enable	Enables the DHCPv6 anti-attack function on the interface.																		
	nfpp dhcpv6-guard policy	Sets the rate-limit threshold and attack threshold.																		
Platform Description	N/A																			

21.89 show nfpp icmp-guard hosts

	Use this command to display the monitored host.	
	show nfpp icmp-guard hosts [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the monitored host.
	<i>vid</i>	The VLAN ID

	<i>interface-id</i>	The interface name
	<i>ip-address</i>	The IP address
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the monitored host. <pre>FS# show nfpp icmp-guard hosts statistics success fail total ----- 100 20 120</pre> The following example displays the monitored host. <pre>FS# show nfpp icmp-guard hosts If column 1 shows '*', it means "hardware failed to isolate host". VLAN interface IP address remain-time(s) --- -</pre>	

21.90 show nfpp icmp-guard summary

	Use this command to display the configuration.	
	show nfpp icmp-guard summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode	

Mode																																		
Usage Guide	N/A																																	
Configuration Examples	The following example displays the configuration. <pre>FS# show nfpp icmp-guard summary</pre> (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.) <table><tr><td>Interface</td><td>Status</td><td>Isolate-period</td><td>Rate-limit</td><td>Attack-threshold</td></tr><tr><td>Global</td><td>Enable</td><td>300</td><td>4/-/60</td><td>8/-/100</td></tr><tr><td>Gi 0/1</td><td>Enable</td><td>180</td><td>5/-/-</td><td>8/-/-</td></tr><tr><td>Gi 0/2</td><td>Disable</td><td>200</td><td>4/-/60</td><td>8/-/100</td></tr></table> Maximum count of monitored hosts: 1000 Monitor period:300s <table><tr><th>Field</th><th>Description</th></tr><tr><td>Interface(Global)</td><td>Global configuration</td></tr><tr><td>Status</td><td>Enables/Disables the anti-attack function.</td></tr><tr><td>Isolate-period</td><td>Isolate period</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr></table>		Interface	Status	Isolate-period	Rate-limit	Attack-threshold	Global	Enable	300	4/-/60	8/-/100	Gi 0/1	Enable	180	5/-/-	8/-/-	Gi 0/2	Disable	200	4/-/60	8/-/100	Field	Description	Interface(Global)	Global configuration	Status	Enables/Disables the anti-attack function.	Isolate-period	Isolate period	Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port	Attack-threshold	In the same format as the rate-limit.
Interface	Status	Isolate-period	Rate-limit	Attack-threshold																														
Global	Enable	300	4/-/60	8/-/100																														
Gi 0/1	Enable	180	5/-/-	8/-/-																														
Gi 0/2	Disable	200	4/-/60	8/-/100																														
Field	Description																																	
Interface(Global)	Global configuration																																	
Status	Enables/Disables the anti-attack function.																																	
Isolate-period	Isolate period																																	
Rate-limit	In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port																																	
Attack-threshold	In the same format as the rate-limit.																																	
Related Commands	Command	Description																																
	icmp-guard attack-threshold	Sets the global attack threshold.																																
	icmp-guard enable	Enables the ICMP anti-attack function.																																
	icmp-guard isolate-period	Sets the global isolate time.																																
	icmp-guard monitor-period	Sets the monitor period.																																
	icmp-guard monitored-host-limit	Sets the maximum number of the monitored hosts.																																
	icmp-guard rate-limit	Sets the global rate-limit threshold.																																
	nfpp icmp-guard enable	Enables the ICMP anti-attack function on the interface.																																
	nfpp icmp-guard isolate-period	Sets the isolate time.																																
	nfpp icmp-guard policy	Sets the rate-limit threshold and attack threshold.																																
Platform Description	N/A																																	

21.91 show nfpp icmp-guard trusted-host

	Use this command to display the trusted host free from being monitored.
	show nfpp icmp-guard trusted-host

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the trusted host free from being monitored. <pre> FS# show nfpp icmp-guard trusted-host IP address mask ----- 1.1.1.0 255.255.255.0 1.1.2.0 255.255.255.0 Total:2 record(s) </pre>	
Related Commands	Command	Description
	icmp-guard trusted-host	Sets the trusted host.
Platform Description	N/A	

21.92 show nfpp ip-guard hosts

	Use this command to display the monitored host.	
	show nfpp ip-guard hosts [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>] [<i>ip-address</i>]]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the monitored host.
	<i>vid</i>	The VLAN ID.
	<i>interface-id</i>	The interface name.
	<i>mac-address</i>	The MAC address.
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A																														
Configuration Examples	The following example displays the monitored host. <pre>FS# show nfpp ip-guard hosts statistics</pre> <table><tr><td>success</td><td>fail</td><td>total</td></tr><tr><td>-----</td><td>----</td><td>----</td></tr><tr><td>100</td><td>20</td><td>120</td></tr></table> The following example displays the monitored host. <pre>FS#show nfpp ip-guard hosts</pre> If column 1 shows '*', it means "hardware do not isolate host" . <table><tr><td>VLAN</td><td>interface</td><td>IP address</td><td>Reason</td><td>remain-time(s)</td></tr><tr><td>----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>1</td><td>Gi0/1</td><td>1.1.1.1</td><td>ATTACK</td><td>110</td></tr><tr><td>2</td><td>Gi0/2</td><td>1.1.2.1</td><td>SCAN</td><td>61</td></tr></table> Total:2 host(s)		success	fail	total	-----	----	----	100	20	120	VLAN	interface	IP address	Reason	remain-time(s)	----	-----	-----	-----	-----	1	Gi0/1	1.1.1.1	ATTACK	110	2	Gi0/2	1.1.2.1	SCAN	61
success	fail	total																													
-----	----	----																													
100	20	120																													
VLAN	interface	IP address	Reason	remain-time(s)																											
----	-----	-----	-----	-----																											
1	Gi0/1	1.1.1.1	ATTACK	110																											
2	Gi0/2	1.1.2.1	SCAN	61																											
Related Commands	Command	Description																													
	clear nfpp ip-guard hosts	Clears the monitored host.																													
Platform Description	N/A																														

21.93 show nfpp ip-guard summary

	Use this command to display the configuration.					
	show nfpp ip-guard summary					
Parameter Description	Parameter		Description			
	N/A		N/A			
Defaults	N/A					
Command Mode	Privileged EXEC mode					
Usage Guide	N/A					
Configuration Examples	The following example displays the configuration.					
	FS# show nfpp ip-guard summary					
	(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)					
	Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold					
	Global	Enable	300	4/-/60	8/-/100	15

	Gi 0/1	Enable	180	5/-/	8/-/	-
	Gi 0/2	Disable	200	4/-/60	8/-/100	20
	Maximum count of monitored hosts: 1000					
	Monitor period..300s					
	Field			Description		
	Interface(Global)			Global configuration		
	Status			Enables/Disables the anti-attack function.		
	Isolate-period			Isolate period		
	Rate-limit			In the format of the rate-limit threshold for the source IP address/ the rate-limit threshold for the source MAC address/ the rate-limit threshold for the port		
Attack-threshold			In the same format as the rate-limit.			
Scan-threshold			Scan threshold			
Related Commands	Command				Description	
	ip-guard attack-threshold				Sets the global attack threshold.	
	ip-guard enable				Enables the IP anti-attack function.	
	ip-guard isolate-period				Sets the global isolate time.	
	ip-guard monitor-period				Sets the monitor period.	
	ip-guard monitored-host-limit				Sets the maximum number of the monitored hosts.	
	ip-guard rate-limit				Sets the global rate-limit threshold.	
	nfpp ip-guard enable				Enables the IP anti-attack function on the interface.	
	nfpp ip-guard isolate-period				Sets the isolate time.	
	nfpp ip-guard policy				Sets the rate-limit threshold and attack threshold.	
Platform Description	N/A					

21.94 show nfpp ip-guard trusted-host

	Use this command to display the trusted host free from being monitored.	
	show nfpp ip-guard trusted-host	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	

Usage Guide	N/A				
Configuration Examples	The following example displays the trusted host free from being monitored. <pre>FS# show nfpp ip-guard trusted-host IP address mask ----- 1.1.1.0 255.255.255.0 1.1.2.0 255.255.255.0 Total.2 record(s)</pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>ip-guard trusted-host</td><td>Sets the trusted host.</td></tr> </table>	Command	Description	ip-guard trusted-host	Sets the trusted host.
Command	Description				
ip-guard trusted-host	Sets the trusted host.				
Platform Description	N/A				

21.95 show nfpp log

	Use this command to display the NFPP log configuration.	
	show nfpp log summary	
	Use this command to display the NFPP log buffer area content.	
	show nfpp log buffer [statistics]	
Parameter Description	Parameter	Description
	statistics	Displays the statistical information of the NFPP log buffer area.
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	When the log buffer area is full, the subsequent logs are to be dropped, and an entry with all attributes "-" is displayed in the log buffer area. The administrator shall increase the capacity of the log buffer area or improve the rate of generating the syslog. The generated syslog in the log buffer area carries with the timestamp, for example: <pre>%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)</pre>	
Configuration Examples	The following example displays the NFPP log configuration. <pre>FS#show nfpp log summary Total log buffer size : 10</pre>	

	Syslog rate : 1 entry per 2 seconds Logging: VLAN 1-3, 5 interface Gi 0/1 interface Gi 0/2 The following example displays the log number in the buffer area. FS#show nfpp log buffer statistics There are 6 logs in buffer. The following example shows the NFPP log buffer area: FS#show nfpp log buffer <table><thead><tr><th>Protocol</th><th>VLAN</th><th>Interface</th><th>IP address</th><th>MAC address</th><th>Reason</th><th>Timestamp</th></tr></thead><tbody><tr><td>ARP</td><td>1</td><td>Gi0/1</td><td>1.1.1.1</td><td>-</td><td>DoS</td><td>2009-05-30 16:23:10</td></tr><tr><td>ARP</td><td>1</td><td>Gi0/1</td><td>1.1.1.1</td><td>-</td><td>ISOLATED</td><td>2009-05-30 16:23:10</td></tr><tr><td>ARP</td><td>1</td><td>Gi0/1</td><td>1.1.1.2</td><td>-</td><td>DoS</td><td>2009-05-30 16:23:15</td></tr><tr><td>ARP</td><td>1</td><td>Gi0/1</td><td>1.1.1.2</td><td>-</td><td>ISOLATE_FAILED</td><td>2009-05-30 16:23:15</td></tr><tr><td>ARP</td><td>1</td><td>Gi0/1</td><td>-</td><td>0000.0000.0001</td><td>SCAN</td><td>2009-05-30 16:30:10</td></tr><tr><td>ARP</td><td>-</td><td>Gi0/2</td><td>-</td><td>-</td><td>PORT_ATTACKED</td><td>2009-05-30 16:30:10</td></tr></tbody></table> <table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Protocol</td><td>ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT</td></tr><tr><td>Reason</td><td>DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED</td></tr></tbody></table>							Protocol	VLAN	Interface	IP address	MAC address	Reason	Timestamp	ARP	1	Gi0/1	1.1.1.1	-	DoS	2009-05-30 16:23:10	ARP	1	Gi0/1	1.1.1.1	-	ISOLATED	2009-05-30 16:23:10	ARP	1	Gi0/1	1.1.1.2	-	DoS	2009-05-30 16:23:15	ARP	1	Gi0/1	1.1.1.2	-	ISOLATE_FAILED	2009-05-30 16:23:15	ARP	1	Gi0/1	-	0000.0000.0001	SCAN	2009-05-30 16:30:10	ARP	-	Gi0/2	-	-	PORT_ATTACKED	2009-05-30 16:30:10	Field	Description	Protocol	ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT	Reason	DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED
Protocol	VLAN	Interface	IP address	MAC address	Reason	Timestamp																																																								
ARP	1	Gi0/1	1.1.1.1	-	DoS	2009-05-30 16:23:10																																																								
ARP	1	Gi0/1	1.1.1.1	-	ISOLATED	2009-05-30 16:23:10																																																								
ARP	1	Gi0/1	1.1.1.2	-	DoS	2009-05-30 16:23:15																																																								
ARP	1	Gi0/1	1.1.1.2	-	ISOLATE_FAILED	2009-05-30 16:23:15																																																								
ARP	1	Gi0/1	-	0000.0000.0001	SCAN	2009-05-30 16:30:10																																																								
ARP	-	Gi0/2	-	-	PORT_ATTACKED	2009-05-30 16:30:10																																																								
Field	Description																																																													
Protocol	ARP, IP, ICMP, DHCP,DHCPv6, NS-NA, RS, RA-REDIRECT																																																													
Reason	DoS, ISOLATED, ISOLATE_FAILE, SCAN, PORT_ATTACKED																																																													
Related Commands	Command					Description																																																								
	clear nfpp log					Clears the NFPP log buffer area.																																																								
Platform Description	N/A																																																													

21.96 show nfpp nd-guard summary

	Use this command to display the configuration.	
	show nfpp nd-guard summary	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command	Privileged EXEC mode	

Mode																		
Usage Guide	N/A																	
Configuration Examples	The following example displays the configuration. <pre>FS# show nfpp nd-guard summary</pre> (Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.) <table><thead><tr><th>Interface</th><th>Status</th><th>Rate-limit</th><th>Attack-threshold</th></tr></thead><tbody><tr><td>Global</td><td>Enable</td><td>20/5/10</td><td>40/10/20</td></tr><tr><td>Gi 0/1</td><td>Enable</td><td>15/15/15</td><td>30/30/30</td></tr><tr><td>Gi 0/2</td><td>Disable</td><td>-/5/30</td><td>-/10/50</td></tr></tbody></table>		Interface	Status	Rate-limit	Attack-threshold	Global	Enable	20/5/10	40/10/20	Gi 0/1	Enable	15/15/15	30/30/30	Gi 0/2	Disable	-/5/30	-/10/50
Interface	Status	Rate-limit	Attack-threshold															
Global	Enable	20/5/10	40/10/20															
Gi 0/1	Enable	15/15/15	30/30/30															
Gi 0/2	Disable	-/5/30	-/10/50															
	<table><thead><tr><th>Field</th><th>Description</th></tr></thead><tbody><tr><td>Interface(Global)</td><td>Global configuration</td></tr><tr><td>Status</td><td>Enables/Disables the anti-attack function.</td></tr><tr><td>Rate-limit</td><td>In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.</td></tr><tr><td>Attack-threshold</td><td>In the same format as the rate-limit.</td></tr></tbody></table>	Field	Description	Interface(Global)	Global configuration	Status	Enables/Disables the anti-attack function.	Rate-limit	In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.	Attack-threshold	In the same format as the rate-limit.							
Field	Description																	
Interface(Global)	Global configuration																	
Status	Enables/Disables the anti-attack function.																	
Rate-limit	In the format of the rate-limit threshold for the NS-NA/RS/RA-REDIRECT.																	
Attack-threshold	In the same format as the rate-limit.																	
Related Commands	<table><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>nd-guard attack-threshold</td><td>Sets the global attack threshold.</td></tr><tr><td>nd-guard enable</td><td>Enables the ND anti-attack function.</td></tr><tr><td>nd-guard rate-limit</td><td>Sets the global rate-limit threshold.</td></tr><tr><td>nfpp nd-guard enable</td><td>Enables the ND anti-attack function on the interface.</td></tr><tr><td>nfpp nd-guard policy</td><td>Sets the rate-limit threshold and attack threshold.</td></tr></tbody></table>	Command	Description	nd-guard attack-threshold	Sets the global attack threshold.	nd-guard enable	Enables the ND anti-attack function.	nd-guard rate-limit	Sets the global rate-limit threshold.	nfpp nd-guard enable	Enables the ND anti-attack function on the interface.	nfpp nd-guard policy	Sets the rate-limit threshold and attack threshold.					
Command	Description																	
nd-guard attack-threshold	Sets the global attack threshold.																	
nd-guard enable	Enables the ND anti-attack function.																	
nd-guard rate-limit	Sets the global rate-limit threshold.																	
nfpp nd-guard enable	Enables the ND anti-attack function on the interface.																	
nfpp nd-guard policy	Sets the rate-limit threshold and attack threshold.																	
Platform Description	N/A																	

21.97 show nfpp nd-guard hosts

	Use this command to display the monitored host. show nfpp nd-guard hosts [statistics [[vlan <i>vid</i>] [interface <i>interface-id</i>]]	
Parameter Description	Parameter	Description
	statistics	Displays the statistics of the monitored host.
	<i>vid</i>	Sets the VLAN ID.
	<i>interface-id</i>	Sets the interface name and number.
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	

Configuration	The following example displays the statistics of the host monitored by ND-guard.																													
Examples	<pre>FS#show nfpp nd-guard hosts statistics</pre> <table><tr><td>success</td><td>fail</td><td>total</td></tr><tr><td>-----</td><td>----</td><td>-----</td></tr><tr><td>10</td><td>2</td><td>12</td></tr></table> The following example displays the host monitored by ND-guard. The “remain-time(s)” refers to the remaining time of isolation. <pre>FS#show nfpp nd-guard hosts</pre> If col_filter 1 shows '*', it means "hardware do not isolate host". <table><tr><td>VLAN</td><td>interface</td><td>ND-guard</td><td>remain-time(s)</td></tr><tr><td>----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>-</td><td>Gi4/2</td><td>ns-na-guard</td><td>174</td></tr><tr><td>-</td><td>Gi4/2</td><td>rs-guard</td><td>98</td></tr><tr><td>-</td><td>Gi4/2</td><td>ra-redirect-guard</td><td>127</td></tr></table> Total: 3 hosts	success	fail	total	-----	----	-----	10	2	12	VLAN	interface	ND-guard	remain-time(s)	----	-----	-----	-----	-	Gi4/2	ns-na-guard	174	-	Gi4/2	rs-guard	98	-	Gi4/2	ra-redirect-guard	127
success	fail	total																												
-----	----	-----																												
10	2	12																												
VLAN	interface	ND-guard	remain-time(s)																											
----	-----	-----	-----																											
-	Gi4/2	ns-na-guard	174																											
-	Gi4/2	rs-guard	98																											
-	Gi4/2	ra-redirect-guard	127																											
Platform	N/A																													
Description																														

21.98 trusted-host

	Use this command to set the trusted hosts free form monitoring. Use the no or default form of this command to restore the default setting,	
	trusted-host { <i>mac mac_mask</i> <i>ip mask</i> <i>IPv6/prefixlen</i> }	
	no trusted-host { all <i>mac mac_mask</i> <i>ip mask</i> <i>IPv6/prefixlen</i> }	
	default trusted-host	
Parameter Description	Parameter	Description
	<i>ip</i>	Sets the IP address
	<i>mac</i>	MAC address
	<i>mac_mask</i>	MAC address mask
	<i>IPv6/prefixlen</i>	IPv6 address and mask length
	<i>mask</i>	IP mask
	all	Deletes the configuration of all trusted hosts with the no form of this command.
Defaults	N/A	
Command Mode	NFPP define configuration mode	
Usage Guide	The administrator can use this command to set the trusted host free from monitoring. The ICMP packets are	

	allowed to be sent to the trusted host CPU without any rate-limit and warning configuration. Configure the mask to set all hosts in one network segment free from monitoring. UP to 500 trusted hosts are supported. Before configuring the trusted-host, the match type must be configured. If the message type configured by the match is Ipv4, the Ipv6 trusted addresses are not allowed. In the same way, if the message type is IPv6, the IPv4 trusted addresses are not allowed.	
Configuration Examples	The following example sets the trusted hosts free form monitoring. <pre>FS(config)# nfpp FS(config-nfpp)# define tcp FS(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255</pre>	
Related Commands	Command	Description
	show nfpp define trusted-host	Displays the trusted host configuration.
Platform Description	N/A	

21.99 no all-guard enable

	Use this command to disable all NFPP guards (except guards self-defined and enabled in interface configuration mode). no all-guard enable	
	Use this command to enable all NFPP guards. all-guard enable	
Parameter Description	Parameter	Description
	N/A	N/A
Command Mode	NFPP configuration mode	
Usage Guide	- By default, all basic NFPP guards are enabled. - This global command supports basic NFPP guards including ARP-GUARD, IP-GUARD, ICMP-GUARD, DHCP-GUARD, DHCPv6-GUARD and ND-GUARD. - The no form command will disable all guards, which is displayed guard-by-guard by using the show running-config command. The exception is guards self-defined and configured in interface configuration mode.	
Configuration Examples	<pre>FS(config)#show running-config begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201</pre>	

	<pre> arp-guard attack-threshold per-port 210 ! FS(config)# nfpp FS(config-nfpp)#no all-guard enable FS(config-nfpp)#show running-config begin nfpp nfpp log-buffer enable no arp-guard enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 no icmp-guard enable no ip-guard enable no dhcp-guard enable no dhcpv6-guard enable no nd-guard enable ! FS(config-nfpp)#all-guard enable FS(config-nfpp)#show running-config begin nfpp nfpp log-buffer enable arp-guard rate-limit per-port 201 arp-guard attack-threshold per-port 210 ! no service password-encryption ! </pre>
Platform	N/A
Description	

22 DoS Protection Commands

22.1 ip deny invalid-l4port

	Use this command to enable the anti-attack of the self-consumption. Use the no form of this command to restore the default setting.	
	ip deny invalid-l4port	
	no ip deny invalid-l4port	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the anti-attack of the self-consumption. <pre>FS(config)# ip deny invalid-l4port</pre> The following example disables the anti-attack of the self-consumption. <pre>FS(config)# no ip deny invalid-l4port</pre>	
Related Commands	Command	Description
	show ip deny invalid-l4port	Displays the state of anti-attack of the self-consumption.
Platform Description	N/A	

22.2 ip deny invalid-tcp

	Use this command to enable the anti-attack of the invalid TCP packets. Use the no form of this command to restore the default setting.	
	ip deny invalid-tcp	
	no ip deny invalid-tcp	

Parameter Description	Parameter	Description
	N/A	N/A
Defaults	The function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration Examples	The following example enables the anti-attack of the invalid TCP packets: <pre>FS(config)# ip deny invalid-tcp</pre> The following example disables the anti-attack of the invalid TCP packets: <pre>FS(config)# no ip deny invalid-tcp</pre>	
Related Commands	Command	Description
	show ip deny invalid-tcp	Displays the state of anti-attack of the invalid TCP packets.
Platform Description	N/A	

22.3 ip deny land

	Use this command to enable the anti-land-attack. Use the no form of this command to restore the default setting.	
	ip deny land	
	no ip deny land	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	This function is disabled by default.	
Command Mode	Global configuration mode	
Usage Guide	N/A	
Configuration	The following example enables the anti-land-attack:	

Examples	FS(config)# ip deny land	
	The following example disables the anti-land-attack: <pre>FS(config)# no ip deny land</pre>	
Related Commands	Command	Description
	show ip deny land	Displays the anti-land-attack state.
Platform Description	N/A	

22.4 show ip deny

	Use this command to display the state of the anti-DOS-attack.	
	show ip deny	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the state of the anti-DOS-attack. <pre>FS#show ip deny Protect against Land attack On Protect against invalid L4port attack Off Protect against invalid TCP attack Off</pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

22.5 show ip deny invalid-l4port

	Use this command to display the state of the anti-consumption-attack.

	show ip deny invalid-l4port	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the state of the anti-consumption-attack. <pre> FS# show ip deny invalid-l4port DoS Protection Mode State ----- protect against invalid l4port attack Off </pre>	
Related Commands	Command	Description
	N/A	N/A
Platform Description	N/A	

22.6 show ip deny invalid-tcp

	Use this command to display the state of the anti-attack of the invalid TCP packets.	
	show ip deny invalid-tcp	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the state of the anti-attack of the invalid TCP packets. <pre> FS# show ip deny invalid-tcp </pre>	

	DoS Protection Mode State ----- protect against invalid tcp attack On	
Related Commands	Command	Description
	ip deny invalid-tcp	Enables the anti-attack of the invalid TCP packets.
Platform Description	N/A	

22.7 show ip deny land

	Use this command to display the anti-land-attack state.	
	show ip deny land	
Parameter Description	Parameter	Description
	N/A	N/A
Defaults	N/A	
Command Mode	Privileged EXEC mode	
Usage Guide	N/A	
Configuration Examples	The following example displays the anti-land-attack state. FS# show ip deny land DoS Protection Mode State ----- protect against land attack On	
Related Commands	Command	Description
	no ip deny land	Enables the anti-land-attack function.
Platform Description	N/A	



 <https://www.fs.com>



The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.