

S5850-24S2Q Switch

CLI Reference Guide

Model: S5850-24S2Q

Contents

Chapter 1 Preface.....	1
1.1 Declaration.....	1
1.2 Audience.....	1
1.3 Conventions.....	1
Chapter 2 Basic Commands.....	2
2.1 System Configuration Commands.....	2
2.2 User Management Commands.....	58
2.3 FTP Commands.....	64
2.4 TFTP Commands.....	72
2.5 scp Commands.....	75
2.6 Telnet Commands.....	79
2.7 SSH Commands.....	82
2.8 Time&Timezone Commands.....	104
2.9 HTTP commands Commands.....	109
Chapter 3 Ethernet Commands.....	122
3.1 Interface Commands.....	122
3.2 Interface Errdisable Commands	144
3.3 MAC Address Table Commands.....	152
3.4 VLAN Commands.....	161
3.5 Voice VLAN Commands.....	175
3.6 Link Aggregation Commands.....	178
3.7 VLAN Classification Commands.....	196
3.8 VLAN Mapping Commands.....	201
3.9 MSTP Commands.....	212
3.10 Flow Control Commands.....	243
3.11 Layer 2 Protocols Tunneling Commands.....	245
3.12 Storm Control Commands.....	251
3.13 Loopback Detection Commands.....	254
3.14 MLAG Commands.....	258

Chapter 4 IP Service Commands.....	294
4.1 ARP Commands.....	294
4.2 DHCP Client Commands.....	312
4.3 DHCP Relay Commands.....	325
4.4 DHCP Server Commands.....	343
4.5 DNS Commands.....	370
Chapter 5 IPv6 Service Commands.....	376
5.1 Tunnel Commands.....	376
5.2 NDP Commands.....	385
5.3 DHCPv6 Relay Commands.....	395
Chapter 6 IP Routing Commands.....	405
6.2 RIP Commands.....	424
6.3 OSPF Commands.....	451
6.4 Route Map Commands.....	511
Chapter 7 IPv6 Routing Commands.....	713
7.1 OSPFv3 Commands.....	713
7.2 RIPng Commands.....	743
7.3 IPv6UC Commands.....	760
7.5 Route Map Commands.....	771
7.6 IPv6 BGP Commands.....	793
Chapter 8 Multicast Commands.....	847
8.2 IGMP Commands.....	851
8.3 IGMP Snooping Commands.....	864
8.4 PIM Commands.....	882
8.5 MVR Commands.....	907
Chapter 9 IPv6 Multicast Commands.....	913
9.2 MLD Commands.....	919
9.3 MLD Snooping Commands.....	939
9.4 PIMv6 Commands.....	964
9.5 MVR6 Commands.....	992

Chapter 10 Traffic Management Commands.....	1001
10.1 QOS Commands.....	1001
Chapter 11 Security Commands.....	1054
11.1 Port Security Commands.....	1054
11.2 Vlan Security Commands.....	1059
11.3 Time Range Commands.....	1062
11.4 ACL Commands.....	1064
11.5 Extend ACL Commands.....	1095
11.6 ACLv6 Commands.....	1120
11.7 Port Group Commands.....	1139
11.8 Vlan Group Commands.....	1141
11.9 COPP Commands.....	1143
11.11 Arp Inspection Commands.....	1184
11.12 DHCP Snooping Commands.....	1204
11.13 IP Source Guard Commands.....	1220
11.14 AAA Commands.....	1223
11.15 RADIUS Authentication Commands.....	1234
11.17 Port Isolate Commands.....	1245
11.18 Private Vlan Commands.....	1248
11.19 DDOS Commands.....	1250
11.20 Key Chain Commands.....	1257
11.22 Device Management Security Commands.....	1263
Chapter 12 IPv6 Security Commands.....	1266
12.1 DHCPv6 Snooping Commands.....	1266
Chapter 13 Reliability Commands.....	1277
13.1 BHM Commands.....	1277
13.2 CPU Traffic Limit Commands.....	1281
13.3 CPU Traffic Statistics Commands.....	1287
13.4 CPU Traffic Protect Commands.....	1294
13.5 UDLD Commands.....	1306

13.6 ERPS Commands.....	1312
13.7 Smart-Link Commands.....	1332
13.8 Multi-Link Commands.....	1348
13.9 Monitor Link Commands.....	1368
13.10 VRRP Commands.....	1374
13.11 Track Commands.....	1386
13.12 VARP Commands.....	1410
13.13 IP BFD Commands.....	1413
Chapter 14 Device Management Commands.....	1426
14.1 STM Commands.....	1426
14.2 Syslog Commands.....	1429
14.3 Mirror Commands.....	1446
14.4 Device Management Commands.....	1466
14.5 Bootrom Commands.....	1473
14.6 Bootup Diagnostic Commands.....	1484
14.7 SmartConfig Commands.....	1486
Chapter 15 Network Management Commands.....	1489
15.1 Network Diagnosis Commands.....	1489
15.2 NTP Commands.....	1491
15.3 Phy Loopback Commands.....	1505
15.4 RMON Commands.....	1512
15.5 SNMP Commands.....	1519
15.6 SFLOW Commands.....	1540
15.7 LLDP Commands.....	1545
Chapter 16 VPN Commands.....	1560
16.1 VRF Commands.....	1560

Chapter 1 Preface

1.1 Declaration

This document updates at irregular intervals because of product upgrade or other reason.

This document is for your reference only.

1.2 Audience

This document is for the following audiences:

- System maintenance engineers
- Debugging and testing engineers
- Network monitoring engineers
- Field maintenance engineers

1.3 Conventions

Command syntax convention table

Syntax	Description
<i>Italic type with capital letters</i>	Use italic type with capital letters for the parameters of the commands. Parameters are the parts which need to replace with the actual value.
(x y ...)	Select one among the choices.
(x y ...)	Select one or none among the choices.
[x y ...]	Select one or more among the choices. The choices can be selected repeatedly.
[x y ...]	Select one or more or none among the choices. The choices can be selected repeatedly.
{x y ...}	Select one or more among the choices. The choices can be selected only once.
{x y ... }	Select one or more or none among the choices. The choices can be selected only once.
<x-y>	Select a number between x and y.

Chapter 2 Basic Commands

2.1 System Configuration Commands

2.1.1 hostname

Command Purpose

To specify or modify the host name for the network server, use the "hostname" command in Global Configuration.

To restore the configuration to the default, use the "no hostname" command.

Command Syntax

hostname *NAME*

no hostname

Parameter	Parameter Description	Parameter Value
NAME	New host name for the network server	Host name is a string with 1-63 characters

Command Mode

Global Configuration

Default

The default host name is Switch.

Usage

The host name is used in prompts and default configuration filenames.

The name must also follow the rules for ARPANET host names. They have as interior characters only letters, digits, hyphens, and underline.

Names must be 64 characters or fewer.

Examples

The following example changes the host name to "sandbox":

```
Switch# configure terminal
Switch(config)# hostname sandbox
sandbox(config)#
```

Related Commands

None

2.1.2 management ip address

Command Purpose

Use this command to set the management IP address on the Switch.

To remove the management IP address, use the no form of this command.

Command Syntax

management ip address (A.B.C.D/M | A.B.C.D mask) (gateway A.B.C.D |)

no management ip address

management ipv6 address (X:X::X:X/M | X:X::X:X mask) (gateway X:X::X:X |)

no management ipv6address

Parameter	Parameter Description	Parameter Value
A.B.C.D/M	The management IPv4 address with mask length configured	IPv4 address with mask length 1-32
A.B.C.D mask	The management IPv4 address and mask configured	IPv4 address and mask
X:X::X:X/M	The management IPv6 address with mask length configured	IPv4 address with mask length 1-128
X:X::X:X mask	The management IPv6 address and mask configured	IPv6 address and mask
gateway A.B.C.D	Add IPv4 gateway	IPv4 address
gateway X:X::X:X	Add IPv6 gateway	IPv6 address

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example sets the management ipv4 address:

```
Switch# configure terminal
```

```
Switch(config)# management ip address 192.168.100.100/24
```

The following example unsets the management ipv4 address:

```
Switch# configure terminal
```

```
Switch(config)# no management ip address
```

The following example sets the management ipv6 address:

```
Switch# configure terminal
```

```
Switch(config)# management ipv6 address 2001:1000::1000/96
```

The following example unsets the management ipv6 address:

```
Switch# configure terminal
```

```
Switch(config)# no management ipv6 address
```


Related Commands

None

2.1.3 management route

Command Purpose

Use this command to set the gateway on the Switch for management ip.

Command Syntax

management route (add | del) gateway A.B.C.D

management ipv6 route (add | del) gateway X:X::X:X

Parameter	Parameter Description	Parameter Value
add	Add the route	-
del	Del the route	-
ipv6	Configure IPv6 gateway	-
gateway	Add gateway	-
A.B.C.D	The IPv4 address of the gateway	IPv4 address
X:X::X:X	The IPv6 address of the gateway	IPv6 address

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example sets the gateway of 192.168.100.254 for the switch:

```
Switch# configure terminal
```

```
Switch(config)# management route add gateway 192.168.100.254
```

The following example sets the gateway of 2001:1000:1 for the switch:

```
Switch# configure terminal
```

```
Switch(config)# management ipv6 route add gateway 2001:1000::1
```

Related Commands

None

2.1.4 show management arp

Command Purpose

Use This command to show the ARP of the management port.

Command Syntax

```
show management arp
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the ARP of the management port:

```
Switch# show management arp
```

Address	Hardware Addr	Interface
10.10.39.241	24:6e:96:62:3f:c4	mgmt-if
10.10.39.254	00:1e:08:09:67:6d	mgmt-if

Related Commands

None

2.1.5 show management ip address

Command Purpose

Use This command to show the IP address of the management port.

Command Syntax

show management ip address
show management ipv6 address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the IP address of the management port:

```
Switch# show management ip address
```

```
Management IP address is: 192.168.100.100/24  
Gateway: 192.168.100.254
```

```
Switch# show management ipv6 address
```

```
Management IPv6 address is: 2001:1000::1000/96  
Gateway: 2001:1000::1
```

Related Commands

None

2.1.6 show management interface

Command Purpose

Use this command to display the configurations and statistics on management interface.

Command Syntax

```
show management interface
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the configurations and statistics on management interface:

```
Switch# show management interface
```

```
Management Interface current state: DOWN
```

```
Description:
```

```
Link encap: Ethernet      HWaddr: 94:EB:AB:88:2A:B4
```

```
Inet addr: 192.168.100.102 Mask: 255.255.255.0
```

```
Bcast: 192.168.100.255    MTU: 1500
```

```
Speed: 10                 Duplex: Half
```

```
Auto-negotiation: Enable
```

```
Received:      2 Packets,      128 Bytes (128.0 b)
```

```
Transmitted:   1 Packets,      78 Bytes (78.0 b)
```

Related Commands

clear counters mgmt-if

2.1.7 clear counters mgmt-if

Command Purpose

Use this command to clear statistics counters on management interface.

Command Syntax

clear counters mgmt-if

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to clear statistics counters on management interface:

```
Switch# clear counters mgmt-if
```

Related Commands

None

2.1.8 enable password**Command Purpose**

Use this command to set the password which is needed when user enter Privileged EXEC mode.

Command Syntax

enable password (privilege LEVEL |) (8 |) LINE

no enable password

Parameter	Parameter Description	Parameter Value
Privilege LEVEL	User privilege level	Level value <1-4>
8	Specifies a hidden password will follow	-
LINE	The password string	-

Command Mode

Global Configuration

Default

None

Usage

If this command is set, user need to provide the password when enter Privileged EXEC mode.

Examples

The following example shows how to set the password:

```
Switch# configure terminal
Switch(config)# enable password 123
Switch(config)# exit
Switch# disable
Switch> enable

Password:
Switch#
```

Related Commands

None

2.1.9 terminal length

Command Purpose

To set the number of lines on the current terminal screen for the current session, use the terminal length command in EXEC mode. To restore the configuration to the default, use the no form of this command.

Command Syntax

terminal length LENGTH

terminal no length

Parameter	Parameter Description	Parameter Value
LENGTH	Number of lines on the screen	The value is a number from 0 to 512. A value of zero disables pausing between screens of output

Command Mode

Privileged EXEC

Default

Automatically detected by terminal screen length by default

Usage

The system uses the length value to determine when to pause during multiple-screen output. A value of zero prevents the switch from pausing between screens of output.

Some types of terminal sessions do not require you to specify the screen length because the screen length specified can be learned by some remote hosts. For example, the rlogin protocol uses the screen length to set up terminal parameters on a remote UNIX host.

Examples

In the following example, the system is configured to prevent output from pausing if it exceeds the length of the screen:

```
Switch# terminal length 0
```

Related Commands

service terminal-length

2.1.10 service terminal-length

Command Purpose

To set the number of lines on the current terminal screen for all sessions, use the service terminal-length command in Global Configuration. To restore the configuration to the default, use the no form of this command.

Command Syntax

service terminal-length LENGTH

no service terminal-length

Parameter	Parameter Description	Parameter Value
LENGTH	Number of lines on the screen	The value is a number from 0 to 512. A value of zero disables pausing between screens of output

Command Mode

Global Configuration

Default

None

Usage

The system uses the length value to determine when to pause during multiple-screen output. A value of zero prevents the switch from pausing between screens of output.

Some types of terminal sessions do not require you to specify the screen length because the screen length specified can be learned by some remote hosts. For example, the rlogin protocol uses the screen length to set up terminal parameters on a remote UNIX host.

Examples

In the following example, the system is configured to prevent output from pausing if it exceeds the length of the screen:

```
Switch# configure terminal
Switch(config)# service terminal-length 0
```

Related Commands

terminal length

2.1.11 banner motd

Command Purpose

To set a single or multiline message banner that appears on the screen when someone logs in to the switch, use the banner motd command in Global Configuration. To restore the configuration to the default, use the no form of this command.

Command Syntax

banner motd line

no banner motd

Parameter	Parameter Description	Parameter Value
LINE	message string	specify a visible character as delimiting character, enter the message between 2 delimiting characters. At most support 99 lines with 1023 character in each line

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to set a single message banner:

```
Switch# configure terminal
```



```
Switch(config)# banner motd #
```

Enter TEXT message. End with the character '#'.

```
this is a example message#
```

Related Commands

banner exec

banner login

2.1.12 banner exec

Command Purpose

To set an exec banner to be displayed on all connected terminals and this banner appears when terminal in Privileged EXEC mode, use the banner motd command in Global Configuration. To restore the configuration to the default, use the no form of this command.

Command Syntax

banner exec line

no banner exec

Parameter	Parameter Description	Parameter Value
LINE	message string	specify a visible character as delimiting character, enter the message between 2 delimiting characters. At most support 99 lines with 1023 character in each line

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to set a single message banner:

```
Switch# configure terminal
```

```
Switch(config)# banner exec #
```

```
Enter TEXT message. End with the character '#'.
this is a example message#
```

Related Commands

banner motd
banner login

2.1.13 banner login

Command Purpose

To set a login banner to be displayed on all connected terminals, and this banner appears after the MOTD banner and before the login prompt, use the banner motd command in Global Configuration. To restore the configuration to the default, use the no form of this command.

Command Syntax

banner login line
no banner login

Parameter	Parameter Description	Parameter Value
LINE	message string	specify a visible character as delimiting character, enter the message between 2 delimiting characters. At most support 99 lines with 1023 character in each line

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to set a single message banner:

```
Switch# configure terminal
Switch(config)# banner login #
```

Enter TEXT message. End with the character '#'.
this is a example message#

Related Commands

banner exec
banner motd

2.1.14 show version

Command Purpose

To display the version information of the hardware and firmware, use the show version command in EXEC mode.

Command Syntax

show version (slot ID |)

Parameter	Parameter Description	Parameter Value
ID	slot id	1-29

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display version information of the hardware and firmware:

```
Switch# show version
```

```
Switch# show version
```

```
NetworkOS Software, Switch, Version 5.3.8.5
```

```
Copyright (C) 2018 Switch Vendor Inc. All rights reserved.
```

```
The current running image is flash:/boot/ulmage.p1010.48t4x.r_20181115
```

```
Switch uptime is 0 days, 19 hours, 8 minutes
```

```
Hardware Type is 52TX
```

Hardware Version is 1.1
SDRAM size 2048M
Flash size 2048M
EPLD Version is 2.1
BootRom Version is 6.1.2
System serial number is E101ZB14202C
Current Web Version is 5.3.8.3

Related Commands

None

2.1.15 line vty

Command Purpose

To set the max login VTY, use this command in Global Configuration. To restore the configuration to the default, use the no form of this command.

Command Syntax

line vty maximum MAX_VTY

no line vty maximum

line vty VTY

Parameter	Parameter Description	Parameter Value
MAX_VTY	Max login VTY	The default value is 8.range <0-8>
VTY	Number of VTY	Range <0-7>

Command Mode

Global Configuration

Default

8

Usage

None

Examples

The following example shows how to set the max VTY to 5:

```
Switch# configure terminal
```

```
Switch(config)# line vty maximum 5
```

The following example shows how to enter Line Configuration mode:

```
Switch# configure terminal
```

```
Switch(config)# line vty 2
```

Related Commands

None

2.1.16 exec-timeout

Command Purpose

To set how much time the login user do not do any operation then the user should be forced to quit, use the no form of this command.

Command Syntax

exec-timeout MINUTES SECONDS

no exec-timeout

Parameter	Parameter Description	Parameter Value
MINUTES	Timeout in minute	Range <0-35791>
SECONDS	Timeout in second	Range <0-2147483>

Command Mode

Line Configuration

Default

600 seconds

Usage

When the user login again then config will be effected

Examples

The following example shows how to set max time the login user do not do any operation then the user should be forced to quit:

```
Switch# configure terminal
```

```
Switch(config)# line vty 0
```

```
Swicth(config-line)# exec-timeout 3 200
```

Related Commands

None

2.1.17 access-class

Command Purpose

To apply IPv4 ACL on line vty. To restore to default, use the no form of this command.

Command Syntax

access-class ACL-NAME in

no access-class in

Parameter	Parameter Description	Parameter Value
ACL-NAME	The name of the IPv4 acl	A string with up to 40 characters

Command Mode

Line Configuration

Default

No ACL

Usage

If an ACL be applied to line VTY, none of the entries in the ACL will be matched except for IP address and port number.

Examples

The following example shows how to apply IPv4 ACL on vty:

```
Switch(config-line)# access-class acl4 in
```

Related Commands

ip access-list

2.1.18 ipv6 access-class

Command Purpose

To apply IPv6 ACL on line vty. To restore to default, use the no form of this command.

Command Syntax

ipv6 access-class ACL-NAME in

no ipv6 access-class in

Parameter	Parameter Description	Parameter Value
ACL-NAME	The name of the IPv6 acl	A string with up to 40 characters

Command Mode

Line Configuration

Default

No ACL

Usage

If an ACL be applied to line VTY, none of the entries in the ACL will be matched except for IP address and port number.

Examples

The following example shows how to apply IPv6 ACL on vty:

```
Switch(config-line)# ipv6 access-class aclv6 in
```

Related Commands

ipv6 access-list

2.1.19 reboot

Command Purpose

To reload the operating system, use the reload command in Privileged EXEC mode.

Command Syntax

reboot

Command Mode

Privileged EXEC

Default

None

Usage

The reboot command halts the system. Use the reboot command after configuration information is entered into a file and saved to the startup configuration.

Examples

The following example is sample dialog from the reboot command:

```
Switch# reboot
```

Related Commands

reload

2.1.20 schedule reboot at

Command Purpose

To schedule a reload of the software to take place at the specified time, use the schedule reboot at command in Global Configuration. To cancel the scheduled reboot task, use the no form of this command.

Command Syntax

schedule reboot at *HH:MM (MM/DD | MM/DD/YYYY | YYYY/MM/DD)*

no schedule reboot

Parameter	Parameter Description	Parameter Value
HH:MM	The hour and minutes	The time range is 00:00 – 23:59
MM/DD	Specify the date for current year (MM/DD format)	date range is [1/1, 12/31]
MM/DD/YYYY	Specify the date (MM/DD/YYYY format, year range is [2000, 2037])	year range is [2000, 2037]
YYYY/MM/DD	Specify the date (YYYY/MM/DD format)	year range is [2000, 2037]

Command Mode

Global Configuration

Default

No scheduled reboot task is defined.

Usage

If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day.

Examples

The following example is sample dialog from the schedule reboot at command:

```
Switch# configure terminal
Switch(config)# schedule reboot at 12:12 2008/12/25
```

Related Commands

schedule reboot delay

2.1.21 schedule reboot delay

Command Purpose

To schedule a reload of the software to take place after the specified time, use the schedule reboot delay command in Global Configuration. To cancel the scheduled reboot task, use the no form of this command.

Command Syntax

schedule reboot delay { HH:MM | MINUTES }

no schedule reboot

Parameter	Parameter Description	Parameter Value
HH:MM	The hour and minutes	The time range is 00:00 – 23:59
MINUTES	The minutes	The range is 1-720

Command Mode

Global Configuration

Default

No scheduled reboot task is defined.

Usage

None

Examples

The following example is sample dialog from the schedule reboot delay command:

```
Switch# configure terminal
Switch(config)# schedule reboot delay 300
```

Related Commands

schedule reboot at

2.1.22 boot system

Command Purpose

To specify the system image that the switch loads at startup, use the following boot system commands in Privileged EXEC mode.

Command Syntax

boot system (tftp: mgmt-if SERVERIP | flash:/) FILE_NAME

Parameter	Parameter Description	Parameter Value
flash:/	System image file for next booting	-
tftp	System image file for next booting	-
mgmt-if	Management port	-
SERVERIP	The tftp server ip	-
FILE_NAME	The file name that will be used to load at startup	The full path and file name, up to 255 characters

Command Mode

Privileged EXEC

Default

None

Usage

Management IP address in startup-config file will be used as source address when system boot via TFTP.

Examples

The following example is sample dialog from the boot system command:

```
Switch# boot system flash:/boot/Internal-1.0.0.25.bin
```

Related Commands

show boot

2.1.23 show boot

Command Purpose

To display the current image and the image the next startup will load, use the show boot command in Privileged EXEC mode.

Command Syntax

```
show boot
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show boot command:

```
Switch# show boot
```

```
The current boot image version is: E330-3.0.0.23.it
```

```
The current running image is: tftp://10.10.29.160/humberOS-e330-ma-v3.0.0.23.it.r.bin
```

```
The next running image is: tftp://10.10.29.160/humberOS-e330-ma-v3.0.0.23.it.r.bin
```

Related Commands

```
show boot images
```

2.1.24 show boot images

Command Purpose

To display all booting images available in the flash system, use the show boot images command in Privileged EXEC mode.

Command Syntax

```
show boot images
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show boot images command:

```
Switch# show boot images
```

System image files list:

Current boot image version: 1.0.0.25

Create Time	Version	File name
=====		
* 2011-07-25 10:58:29	v3.0.0.22it	Internal-.00.22.bin

Related Commands

show boot

2.1.25 show memory

Command Purpose

To display memory utilization information about the active processes, use the show memory command in Privileged EXEC mode.

Command Syntax

show memory (all | bgp | bhm | chsm | dhclient | dot1x | imi | ipv6 | lacp | ldp | lib | mstp | nsm | oamd | onmd | ospf | pim | ptp | rip | rsvp | shal | summary)

Parameter	Parameter Description	Parameter Value
all	All memory information	-
bgp	Border Gateway Protocol (BGP)	-
bhm	Health monitoring	-
chsm	Chassis management	-
dhclient	DHCP client module	-
dhcpd	DHCP	-
dhcprelay	DHCP relay	-
dhcprelay6	DHCP relay6(IPv6)	-

Parameter	Parameter Description	Parameter Value
dot1x	IEEE 802.1X Port-Based Access Control	-
imi	Integrated Management Interface (IMI)	-
ipv6	Internet Protocol version 6 (IPv6)	-
lACP	Link Aggregation Control Protocol (LACP)	-
ldp	Label Distribution Protocol (LDP)	-
lib	Library information	-
mstp	Spanning Tree Protocols (STP/RSTP/MSTP)	-
nsm	Network Service Module (NSM)	-
oamd	Bidirectional Forwarding Detection (BFD)	-
onmd	LLDP and EFM_OAM	-
ospf	Open Shortest Path First (OSPF)	-
pim	Protocol Independent Multicast (PIM)	-
ptp	Precision Time Protocol (PTP)	-
rip	Routing Information Protocol (RIP)	-
rsvp	Resource Reservation Protocol (RSVP)	-
shal	Hal server monitoring	-
summary	Summary memory information	-
monitor	monitor	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show memory command with keyword bgp:

```
Switch# show memory bgp
```

Library memories for BGP

Memory type		Alloc cells	Alloc bytes
=====			
Temporary memory	:	6596	322216
Hash	:	10	320
Hash index	:	10	40960
Hash bucket	:	55	880
Link list	:	13	400

Link list node	:	115	1840
Show	:	1	512
Show page	:	1	8192
Show server	:	1	64
Prefix IPv4	:	6	48
Route table	:	6	48
Route node	:	309	19776
Vector	:	3383	324768
Vector index	:	3383	48824
SNMP subtree	:	8	6144
Host config	:	1	16
Message of The Day	:	1	128
IMI Client	:	2	1056
VTY master	:	1	16
VTY if	:	52	39936
VTY connected	:	3	192
Message handler	:	2	128
Host	:	1	96
Log information	:	2	128
Context	:	1	512
Memories for BGP			
Memory type		Alloc cells	Alloc bytes
=====			
BGP structure	:	1	768
BGP VR structure	:	1	384
BGP global structure	:	1	64
BGP peer	:	1	2048
Ext community	:	1	16
BGP as list master	:	1	32
Community list handler	:	1	32
BGP Damp Reuse List Array	:	1	2048
BGP table	:	31	248
BGP VRF list	:	1	64

Related Commands

show processes memory sorted

2.1.26 show cpu traffic-limit

Command Purpose

Use this command to show the CPU traffic-limit configurations.

Command Syntax

show cpu traffic-limit

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show cpu traffic-limit :

```
Switch# show cpu traffic-limit
```

reason	rate (pps)	class
bpdu	64	3
cfm	512	2
slow-protocol	128	1
eapol	128	0
erps	128	2
smart-link	128	2
udld	128	3
arp	640	1
dhcp	128	0
rip	64	1
ldp	512	1
ospf	256	1
pim	128	1
vrrp	512	1
rsvp	512	1
ipda	1024	0
icmp-redirect	128	0
mcast-rpf-fail	128	1
macsa-mismatch	128	0
port-security-discard	128	0
vlan-security-discard	128	0

mtu-dontfrag	64	0
mtu-frag	64	0
ptp	512	2
ip-option	512	0
ucast-ttl-fail	64	0
mpls-ttl-fail	64	0
igmp	128	2
sflow-ingress	128	0
sflow-egress	128	0
fwd-to-cpu	64	0
mpls-tp-pwoam	128	2
Total rate:	2048 (pps)	

Related Commands

2.1.27 show processes cpu sorted

Command Purpose

To display CPU utilization information about the active processes sorted by percentage in a device, use the show processes cpu sorted command in Privileged EXEC mode.

Command Syntax

```
show process cpu sorted
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show process cpu sorted :

```
Switch# show processes cpu sorted
```

PID	TIME	%CPU	TTY	COMMAND

924 00:20:03	2.0 ?	hsrpd
956 00:07:17	0.7 ?	nsm
1007 00:02:44	0.2 ?	imi
959 00:01:24	0.1 ?	snmpd
1317 00:00:01	0.1 pts/0	imish
5 00:00:45	0.0 ?	events/0
983 00:00:23	0.0 ?	mstpd
985 00:00:15	0.0 ?	onmd
966 00:00:15	0.0 ?	lcpd
963 00:00:12	0.0 ?	bhm
929 00:00:12	0.0 ?	chsm
964 00:00:11	0.0 ?	oamd
919 00:00:10	0.0 ?	ntpd
1003 00:00:08	0.0 ?	pimd
942 00:00:08	0.0 ?	sshd
957 00:00:08	0.0 ?	dhcrelay
973 00:00:07	0.0 ?	authd
1005 00:00:07	0.0 ?	ldpd
977 00:00:07	0.0 ?	rmond
1021 00:00:07	0.0 ?	ripd
1027 00:00:07	0.0 ?	ospfd
1032 00:00:07	0.0 ?	bgpd
1 00:00:05	0.0 ?	init
779 00:00:04	0.0 ?	jffs2_gcd_mtd1
1106 00:00:01	0.0 ?	imish
3 00:00:00	0.0 ?	ksoftirqd/0
916 00:00:00	0.0 ?	syslog-ng
65 00:00:00	0.0 ?	bdi-default
965 00:00:00	0.0 ?	ptpd
917 00:00:00	0.0 ?	crond
63 00:00:00	0.0 ?	sync_supers
1096 00:00:00	0.0 ?	telnetd
6 00:00:00	0.0 ?	khelper
105 00:00:00	0.0 ?	khungtaskd
2 00:00:00	0.0 ?	kthreadd
4 00:00:00	0.0 ?	watchdog/0
9 00:00:00	0.0 ?	netns
10 00:00:00	0.0 ?	async/mgr
66 00:00:00	0.0 ?	kblockd/0
73 00:00:00	0.0 ?	kseriod
88 00:00:00	0.0 ?	rpciod/0
106 00:00:00	0.0 ?	kswapd0
157 00:00:00	0.0 ?	aio/0
164 00:00:00	0.0 ?	nfsiod

171 00:00:00	0.0 ?	crypto/0
712 00:00:00	0.0 ?	mtddbckd
741 00:00:00	0.0 ?	kpsmoused
789 00:00:00	0.0 ?	PETH/Tx
912 00:00:00	0.0 ?	angel
1098 00:00:00	0.0 ?	telnetd
1414 00:00:00	0.0 pts/0	imish
1415 00:00:00	0.0 pts/0	more
1416 00:00:00	0.0 ?	ps

Related Commands

None

2.1.28 show processes cpu history

Command Purpose

To display CPU utilization information for a period of time, use the show processes cpu history command in Privileged EXEC mode, the period of 1s, 1min, 5min could be shown.

Command Syntax

```
show process cpu history
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show processes cpu history command:

```
Switch# show processes cpu history
```

```
CPU usage for five seconds: 4.17%; one minute: 3.70%; five minutes: 3.68%
```

Related Commands

None

2.1.29 show processes memory sorted

Command Purpose

To display memory utilization information about the active processes sorted by percentage in a device, use the show processes memory sorted command in Privileged EXEC mode. Here, CPU usage for each process means the CPU timeslice used by this process from the process was started to this command has been operated.

Command Syntax

show processes memory sorted (core | physical | virtual)

Parameter	Parameter Description	Parameter Value
core	Size in physical pages of the core image of the process	-
physical	Non-swapped physical memory that a task has used	-
virtual	Virtual memory usage of entire process	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show processes memory sorted command without keywords:

```
Switch# show processes memory sorted

Total: 256108; Used: 89644; Free: 166464; Buffers: 0
  PID TTY      RSS    VSZ    SZ COMMAND
1317 pts/0    9516  13104  3276 imish
1106 ?         9428  13104  3276 imish
1463 pts/0    7436  13104  3276 imish
 956 ?         6836  14644  3661 nsm
```

1007 ?	5948	9624	2406 imi
924 ?	5912	17652	4413 hrsrvd
959 ?	3336	8076	2019 snmpd
1032 ?	2724	8204	2051bgpd
1027 ?	2488	7140	1785 ospfd
1003 ?	2472	7152	1788 pimd
957 ?	2340	6572	1643 dhcrelay
983 ?	2336	6592	1648 mstpd
1021 ?	2324	6600	1650 ripd
1005 ?	2320	6732	1683 ldpd
942 ?	2284	6772	1693 sshd
985 ?	2208	6592	1648 onmd
929 ?	2132	7168	1792 chsm
966 ?	2028	6140	1535 lacpd
973 ?	2028	6284	1571 authd
965 ?	2024	6408	1602 ptpd
964 ?	1952	6364	1591 oamd
977 ?	1948	6200	1550 rmond
963 ?	1708	5980	1495 bhm
919 ?	1120	3792	948 ntpd
916 ?	1060	2300	575 syslog-ng
1465 pts/0	764	2516	629 ps
917 ?	668	3040	760 crond
1 ?	656	2928	732 init
1464 pts/0	472	1668	417 more
1096 ?	416	2928	732 telnetd
1098 ?	272	2928	732 telnetd
912 ?	172	1496	374 angel
2 ?	0	0	0 kthreadd
3 ?	0	0	0 ksoftirqd/0
4 ?	0	0	0 watchdog/0
5 ?	0	0	0 events/0
6 ?	0	0	0 khelper
9 ?	0	0	0 netns
10 ?	0	0	0 async/mgr
63 ?	0	0	0 sync_supers
65 ?	0	0	0 bdi-default
66 ?	0	0	0 kblockd/0
73 ?	0	0	0 kseriod
88 ?	0	0	0 rpciod/0
105 ?	0	0	0 khungtaskd
106 ?	0	0	0 kswapd0
157 ?	0	0	0 aio/0
164 ?	0	0	0 nfsiod

171 ?	0	0	0 crypto/0
712 ?	0	0	0 mtdblockd
741 ?	0	0	0 kpsmoused
779 ?	0	0	0 jffs2_gcd_mtd1
789 ?	0	0	0 PETH/Tx

Related Commands

None

2.1.30 terminal monitor

Command Purpose

To copy debug output to the current terminal line, use the terminal monitor command in Privileged EXEC mode.

Command Syntax

terminal monitor

terminal no monitor

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the terminal monitor command:

```
Switch# terminal monitor
```

```
Jan  1 16:09:30 DUT1 IMISH-6: ready to service
```

Related Commands

None

2.1.31 configure terminal

Command Purpose

To enter Global Configuration, use configure terminal command in Privileged EXEC mode.

Command Syntax

configure terminal

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to enter Global Configuration. Note that commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).

After you enter the configure command, the system prompt changes from # to (config)#, indicating that the switch is in Global Configuration. To leave Global Configuration and return to Privileged EXEC mode, type end or press Ctrl-Z.

Examples

In the following example, the user enters Global Configuration:

```
Switch# configure terminal
```

```
Switch(config)#
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#
```

Related Commands

enable

disable

2.1.32 disable

Command Purpose

To exit Privileged EXEC mode and return to user EXEC mode, enter the disable command in EXEC mode.

Command Syntax

disable

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the user enters Privileged EXEC mode using the enable command, then exits back to user EXEC mode using the disable command. Note that the prompt for user EXEC mode is >, and the prompt for Privileged EXEC mode is #:

```
Switch# configure terminal
Switch> enable

Password: <password>
Switch# disable
Switch>
```

Related Commands

Enable

2.1.33 enable

Command Purpose

To enter Privileged EXEC mod, use the enable command in user EXEC or Privileged EXEC mode.

Command Syntax

enable

Command Mode

User EXEC

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the user enters Privileged EXEC mode using the enable command. The system prompts the user for a password before allowing access to the Privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the disable command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for Privileged EXEC mode is the number sign (#).:

```
Switch# configure terminal
```

```
Switch> enable
```

```
Password: <password>
```

```
Switch# disable
```

```
Switch>
```

Related Commands

Disable

2.1.34 end

Command Purpose

To end the current configuration session and return to Privileged EXEC mode, use the end command in Global Configuration.

Command Syntax

end

Command Mode

Global Configuration

Default

None

Usage

This command will bring you back to Privileged EXEC mode regardless of what configuration mode or configuration sub-mode you are in.

This global configuration command can be used in any configuration mode.

Use this command when you are done configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

In the following example, the end command is used to exit from interface configuration mode and return to Privileged EXEC mode. A show command is used in Privileged EXEC mode to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# end
Switch# show interface eth-0-1
```

Related Commands

Exit

2.1.35 exit (global)

Command Purpose

To exit any configuration mode to the lower mode in the CLI mode hierarchy, use the exit command in any configuration mode.

Command Syntax

exit

Command Mode

All Configuration Mode

Default

None

Usage

The exit command is used in the CLI to exit from the current command mode to the lower mode in the CLI mode hierarchy.

For example, use the exit command in Global Configuration to return to Privileged EXEC mode. Use the exit command in interface, line, or router configuration mode to return to Global Configuration.

Examples

The following example displays an exit from the interface configuration mode to return to the Global Configuration:

```
Switch# configure terminal
Switch(config-if)# exit
Switch(config)#
```

Related Commands

end

exit (EXEC)

2.1.36 exit (EXEC)

Command Purpose

To close an active terminal session by logging off the switch, use the exit command in EXEC mode.

Command Syntax

exit

Command Mode

Privileged EXEC

Default

None

Usage

Use the exit command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

Examples

In the following example, the exit (global) command is used to move from Global Configuration to Privileged EXEC mode, the disable command is used to move from Privileged EXEC mode to user EXEC mode, and the exit (EXEC) command is used to log off (exit the active session):

```
Switch# configure terminal
Switch(config)# exit
```

```
Switch# disable  
Switch> exit
```

Related Commands

Quit

2.1.37 quit

Command Purpose

To close an active terminal session by logging off the switch, use the quit command in EXEC mode.

Command Syntax

quit

Command Mode

All Configuration Mode

Default

None

Usage

Use the quit command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

Examples

In the following example, the quit command is used to move from Global Configuration to Privileged EXEC mode, the disable command is used to move from Privileged EXEC mode to user EXEC mode, and the quit command is used to log off (exit the active session):

```
Switch# configure terminal  
Switch(config)# quit  
Switch# disable  
Switch> quit
```

Related Commands

Exit

2.1.38 cd

Command Purpose

Change the current directory to dir, use the cd command in EXEC mode.

Command Syntax

cd (dir |)

Parameter	Parameter Description	Parameter Value
dir	(Optional) The directory or file systems followed by a colon. If flash: argument is specified, change the current directory to flash: . If udisk: argument is specified, change the current directory to udisk:. If you don't use USB device, failed to cd udisk	-

Command Mode

Privileged EXEC

Default

The initial default file system is flash:. If you do not specify a directory on a file system, the default is the root directory on that file system.

Usage

For all EXEC commands that have an optional file system argument, the system uses the file system specified by the cd command when you omit the optional file system argument. For example, the dir EXEC command, which displays a list of files on a file system, contain an optional file system argument. When you omit this argument, the system lists the files on the file system specified by the cd command.

Examples

In the following example, the cd command is used to set the default file system to the Flash memory.:

```
Switch# configure terminal
DUT1# cd
DUT1# pwd
flash:/
```

In the following example, the cd command is used to set the default file system to the USB device:

```
Switch# configure terminal
storage device
DUT1# cd udisk:
DUT1# pwd
udisk:/
```

In the following example, the cd command is used to set the file system without plug in the USB mass storage device:

```
Switch# cd udisk:
```

```
% Failed to cd udisk:: No such file or directory
```

In the following example, the cd command is used to set the file system with plug in the USB mass storage device

Related Commands

dir

ls

Pwd

2.1.39 copy

Command Purpose

To copy file system, use the copy command in Privileged EXEC mode.

Command Syntax

copy source-name destination-name

Parameter	Parameter Description	Parameter Value
source-name	The location URL of the source file to be copied. The source can be either local or remote	-
destination-name	The destination URL of the copied file. The destination can be either local or remote	-

Command Mode

Privileged EXEC

Default

None

Usage

The exact format of the source and destination URLs varies according to the file or directory location. You may enter a particular file or a filename that follows the standard file system syntax (filesystem:[/filepath][/filename]).

Examples

The following example shows how to get image from TFTP server through in band management interface.:

```
Switch# copy tftp://192.168.0.1/image flash:/boot/image
```

Download from URL to temporary file.

Get file from tftp://192.168.0.1/image

.....
Received 15591515 bytes in 16.6 seconds

Copy the temporary file to its destination.

.....
15591515 bytes in 69.8 seconds, 218 kbytes/second

The following example shows how to get image from TFTP server through out band management interface:

Switch# copy mgmt-if tftp://192.168.0.1/image flash:/boot/image

Related Commands

Delete

2.1.40 delete

Command Purpose

To delete a file on the flash, use the delete command in Privileged EXEC mode.

Command Syntax

delete file-name

Parameter	Parameter Description	Parameter Value
file-name	The file name that is supposed to be deleted	-

Command Mode

Privileged EXEC

Default

None

Usage

If you attempt to delete the configuration file or image, the system prompts you to confirm the deletion. Also, if you attempt to delete the system specified file such as DHCP snooping bindings, the system prompts you to confirm the deletion.

Examples

The following example deletes the file named test from the flash:

Switch# delete flash:/test

```
Are you sure to delete flash:/test? [confirm]:y
```

Related Commands

Copy

2.1.41 dir

Command Purpose

To display a list of files on a file system, use the dir command in EXEC mode.

Command Syntax

dir (flash: | udisk: |) (directory-name |) (file-name |)

Parameter	Parameter Description	Parameter Value
flash	The flash system	-
udisk	The USB mass storage device. If you don't use USB mass storage device, failed to dir udisk	-
directory-name	The directory in flash or udisk	-
file-name	The file name	-

Command Mode

Privileged EXEC

Default

None

Usage

Use the dir (Flash file system) command to display flash or udisk information.

Examples

The following is sample output from the dir command.:

```
Switch# dir
```

```
Directory of flash:/
```

```
total 42
```

```
drwxr-xr-x  2    0 Jul 30 15:42 boot
```

```
drwxr-xr-x  3    0 Jan  1  1970 conf
```

```
drwxr-xr-x  2    0 Jan  1  1970 log
```

```
-rw-r----- 1 1020 Jul 29 19:18 startup-config.conf
```

```
-rw-r--r--  1 10270 Jul 30 10:10 syslog
-rw-r--r--  1  6886 Jul 29 23:59 syslog.1.gz
63.0M bytes total (30.4M bytes free)
Switch # cd udisk:
Switch # dir
Directory of udisk:/
total 12
drwxrwxrwx 2 4096 Jun  2  2011 test
drwxrwxrwx 2 4096 Jun  8  2011 test1
drwxrwxrwx 2 4096 Jun  7  2011 test2
3.7G bytes total (3.7G bytes free)
```

The following is sample output from udisk if plug in the USB mass storage device.:

```
Switch# cd udisk:
Switch# dir

Directory of udisk:/

total 12
drwxrwxrwx 2 4096 Jun  2  2011 test
drwxrwxrwx 2 4096 Jun  8  2011 test1
drwxrwxrwx 2 4096 Jun  7  2011 test2
3.7G bytes total (3.7G bytes free)
```

Related Commands

ls

2.1.42 ls

Command Purpose

To display a list of files on a file system, use the ls command in EXEC mode.

Command Syntax

ls (flash: | udisk: |) (directory-name |) (file-name |)

Parameter	Parameter Description	Parameter Value
flash	The flash system	-
udisk	The USB mass storage device. If you don't use USB mass storage device, failed to dir udisk	-
directory-name	The directory in flash or udisk	-
file-name	The file name	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the ls command:

```
Switch# ls

Directory of flash:/
total 42
drwxr-xr-x  2    0 Jul 30 15:42 boot
drwxr-xr-x  3    0 Jan  1  1970 conf
drwxr-xr-x  2    0 Jan  1  1970 log
-rw-r----- 1 1020 Jul 29 19:18 startup-config.conf
-rw-r--r--  1 10270 Jul 30 10:10 syslog
-rw-r--r--  1  6886 Jul 29 23:59 syslog.1.gz
63.0M bytes total (30.4M bytes free)
```

Related Commands

dir

2.1.43 more

Command Purpose

To display the contents of a file, use the more command in EXEC mode.

Command Syntax

more (flash: | udisk:) (directory-name |) file-name

Parameter	Parameter Description	Parameter Value
flash	The flash system	-
udisk	The USB mass storage device. If you don't use USB mass storage device, failed to dir udisk	-
directory-name	The directory in flash or udisk	-
file-name	The file name	-

Command Mode

Privileged EXEC

Default

None

Usage

The system can only display a file in ASCII format.

Examples

The following partial sample output displays the configuration file named startup-config in flash:

```
Switch# more flash:/startup-config.conf
```

Related Commands

dir

ls

2.1.44 mkdir**Command Purpose**

To create a new directory in a Flash file system or udisk device, use the mkdir command in EXEC mode.

Command Syntax

mkdir directory-name

Parameter	Parameter Description	Parameter Value
directory-name	The directory in flash or udisk	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems.

Examples

The following example creates a directory named newdir in Flash.:

```
Switch# mkdir flash:/newdir
```

The following example creates a directory named newdir in USB mass storage device if plug in it:

```
Switch# mkdir udisk:/newdir
```

Related Commands

rmdir

dir

2.1.45 rename

Command Purpose

To rename a file in a Class C Flash file system or udisk device, use the rename command in EXEC mode.

Command Syntax

rename old-filename new-filename

Parameter	Parameter Description	Parameter Value
old-filename	The original file name in flash	-
new-filename	The new file name in flash	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems

Examples

In the following example, the file named startup-config.conf-bak is renamed startup-config.conf-bak2:

```
Switch# configure terminal
```

```
Switch1# rename udisk:/wus udisk:/wu
```

```
Are you sure to rename udisk:/wus? [confirm]
```

Related Commands

2.1.46 rmdir

Command Purpose

To remove an existing directory in a Flash file system or udisk device, use the rmdir command in Privileged EXEC mode.

Command Syntax

rmdir directory-name

Parameter	Parameter Description	Parameter Value
directory-name	The directory in flash	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is valid only for local file systems

Examples

The following example deletes a directory named newdir:

```
Switch# rmdir flash:/newdir
```

```
Are you sure to delete newdir? [yes/no]: y
```

Related Commands

mkdir

dir

2.1.47 tar create

Command Purpose

To create an new tar file in a Flash file system or udisk device, use the tar create command in Privileged EXEC mode.

Command Syntax

tar create tar-file-name source-directory

Parameter	Parameter Description	Parameter Value
tar-file-name	The file name of the new tar file	-
source-directory	The source directory in flash	-

Command Mode

Privileged EXEC

Default

None

Usage

The source-directory must be a directory

Examples

The following example creates a tar file named tar1:

```
Switch# tar create udisk:/tar1 udisk:/wu
```

Related Commands

tar table

tar xtract

2.1.48 tar table

Command Purpose

To display files in the tar file, use the tar table command in Privileged EXEC mode.

Command Syntax

tar table tar-file-name

Parameter	Parameter Description	Parameter Value
tar-file-name	The file name of the new tar file	-

Command Mode

Privileged EXEC

Default

None

Usage

The tar-file-name must be a in the flash

Examples

The following example shows files in a tar file named tar1:

```
Switch# tar table udisk:/tar1
```

Related Commands

tar create

2.1.49 tar xtract

Command Purpose

To untar files in the tar file, use the tar xtract command in Privileged EXEC mode.

Command Syntax

tar xtract tar-file destination-directory

Parameter	Parameter Description	Parameter Value
tar-file	The file name of the tar file	-
destination-directory	The destination directory	-

Command Mode

Privileged EXEC

Default

None

Usage

The destination-directory must exist in the flash. You can use mkdir to create a new directory.

Examples

The following shows an example to extract a tar file named tar1 into a directory name dir1:

```
Switch# tar xtract flash:/tar1 flash:/mydir
```

Related Commands

tar create

tar table

2.1.50 show diagnostic-information

Command Purpose

Display diagnostic-information including syslog files, core dump files, tcam entries ,running-config, startup-config, version, clock, memory and logging buffer.

Command Syntax

show diagnostic-information (bgp | ospf |)

Parameter	Parameter Description	Parameter Value
bgp	BGP protocol diagnostic information	-
ospf	OSPF protocol diagnostic information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example show diagnostic-information:

```
Switch# show diagnostic-information
```

Related Commands

None

2.1.51 tar diagnostic-information

Command Purpose

To put diagnostic-information to a Flash file system ,udisk device, ftp server or tftp server, use the tar diagnostic-information command in Privileged EXEC mode. Syslog files, core dump files, tcam entries, running-config, startup-config, version, clock, memory and logging buffer are included in this tarfile.

Command Syntax

tar diagnostic-information (mgmt-if |) destination-directory/ tar-file

Parameter	Parameter Description	Parameter Value
destination-directory	The destination directory, such as flash, udisk, tftp or ftp server	-
tar-file	The file name of the tar file	-

Command Mode

Privileged EXEC

Default

None

Usage

The destination-directory must reachable and disk is enough

Examples

The following shows an example to put a diagnostic-information tar file to flash:

```
Switch# tar diagnostic-information flash:/diag.tar.gz
```

Related Commands

None

2.1.52 format

Command Purpose

To format udisk, all data on udisk: will be lost.

Command Syntax

format udsik:

Parameter	Parameter Description	Parameter Value
udsik:	The USB mass storage device. If you don't use USB mass storage device, failed to format udisk	-

Command Mode

Application Configuration

Default

None

Usage

The destination-directory must exist

Examples

The following shows an example to format USB mass storage device:

```
Switch# configure terminal
```

```
Switch(config)# format udisk:
```

```
WARNING: All data on udisk: will be lost!!!
```

```
And format operation may take a while.
```

```
Are you sure to process with format? [yes/no]: yes
```

Related Commands

None

2.1.53 umount

Command Purpose

To uninstall the USB mass storage device before plug out it from the switch.

Command Syntax

umount udsik:

Parameter	Parameter Description	Parameter Value
udisk:	The USB mass storage device. If you don't use USB mass storage device, failed to format udisk	-

Command Mode

Application Configuration

Default

None

Usage

USB mass storage device must exist in the system. You can use umount command to uninstall the USB mass storage device.

Examples

The following shows an example to umount USB mass storage device:

```
Switch# configure terminal
```

```
Switch(config)# umount udsik:
```

After this operation, you can not use USB disk.

```
Are you sure to continue? [yes/no]: yes
```

Related Commands

None

2.1.54 cut-through enable

Command Purpose

To enable cut through mode, and can configure speed only on GG truck .

Command Syntax

```
cut_through_forwarding enable ( 10G-40G-100G | 1G-10G-100G | 1G-10G-40G | )
```

```
no cut_through_forwarding enable
```

Parameter	Parameter Description	Parameter Value
enbale	enable cut through mode	-
(10G-40G-100G 1G-10G-100G 1G-10G-40G)	Configure cut_through speed	-

Command Mode

Application Configuration

Default

10G-40G-100G

Usage

None

Examples

The following example shows how to configure cut through mode:

```
Switch# configure terminal
```

```
Switch(config)# cut-through-forwarding enable 1G-10G-40G
```

```
% Configuration about cutting through forwarding mode has been stored, but cannot take effect until the next reload.
```

Related Commands

None

2.1.55 show cut-through-forwarding mode

Command Purpose

To display current working mode.

Command Syntax

```
show cut-through-forwarding mode
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following shows an example to display current working mode:

```
DUT1# show cut-through-forwarding mode
```

Related Commands

2.1.56 reset factory-config

Command Purpose

Reset to factory configuration.

Command Syntax

```
reset factory-config
```

Command Mode

Privileged EXEC

Default

None

Usage

Device will restore the saved configuration to factory configuration when select yes, and prompt to save configuration when rebooting, please select NO.

Examples

The following shows an example to reset factory configuration:

```
Switch# configure terminal
```

```
DUT1# reset factory-config
```

This action will reset the saved configuration immediately.
Running-config will be erased after reboot. Continue? [yes/no]:

Related Commands

None

2.1.57 show factory-config

Command Purpose

To display the factory configuration.

Command Syntax

```
show factory-config
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following shows an example to display factory configuration DUT1# show factory-config :

```
DUT1# show factory-config
```

Related Commands

None

2.1.58 show this

Command Purpose

To display the configuration of this mode.

Command Syntax

show this

Command Mode

All Configuration Mode

Default

None

Usage

Not support this mode: key-chain, key-chain key, time range, acl, route-map, line, class map

Examples

The following example show the configuration of this mode:

```
Switch(config-vlan)# show this
```

```
vlan database
```

```
  vlan 5
```

```
!
```

Related Commands

None

2.1.59 show route-mac

Command Purpose

To display the route MAC address of this device.

Command Syntax

show route-mac

Command Mode

Privileged EXEC

Default

None

Usage

All interfaces on a device share the same single route-mac.

Examples

The following shows an example to display route-mac of this device:

```
Switch# show route-mac
```

```
Route MAC is: 222c.12fd.6c00
```

```
!
```

Related Commands

None

2.2 User Management Commands

2.2.1 username

Command Purpose

Use this command to create or delete a local user account on the switch.

Command Syntax

username WORD

no username WORD

Parameter	Parameter Description	Parameter Value
username	Establish User Name Authentication	-
WORD	User name	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to add a user named testName:

```
Switch# configure terminal
Switch(config)#username testName
```

Related Commands

None

2.2.2 username password

Command Purpose

Use this command to add username and password.

Command Syntax

username *WORD* password (8 |) LINE

Parameter	Parameter Description	Parameter Value
WORD	User name	-
Password	Password for username	-
(8)	Specifies a hidden password will follow	-
LINE	User password string	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to add a user named testName and with the password of 123456:

```
Switch# configure terminal
```



```
Switch(config)# username testName password 123456
```

Related Commands

None

2.2.3 username secret

Command Purpose

Use this command to add username and password and the password will be encrypted by the switch.

Command Syntax

username WORD secret LINE

Parameter	Parameter Description	Parameter Value
WORD	User name	-
secret	Specify the secret for the user	-
LINE	User privilege level	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to add a user named testName and with the password of 123456:

```
Switch# configure terminal
```

```
Switch(config)#username testName secret 123456
```

Related Commands

2.2.4 username privilege

Command Purpose

Use this command to set a local user account with privilege level on the switch.

Command Syntax

username WORD privilege <1-4>

Parameter	Parameter Description	Parameter Value
username WORD	User name	-
privilege <1-4>	ser privilege level	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to add a user with privilege level of 2:

```
Switch# configure terminal
```

```
Switch(config)#username testName privilege 2
```

Related Commands

None

2.2.5 username service-type

Command Purpose

Use this command to set the user service type.

Command Syntax

username WORD service-type ({ rpc-api | ssh | telnet | web } | all | none)

Parameter	Parameter Description	Parameter Value
username WORD	User name	-
service-type	User service type(include rpc-api, ssh, telnet, web)	-

Command Mode

Global Configuration

Default

Allow all user service type

Usage

None

Examples

This is a sample show how to set only support rpc-api user service-type:

```
Switch# configure terminal
```

```
Switch(config)#username testName service-type rpc-api
```

Related Commands

None

2.2.6 username privilege password**Command Purpose**

Use this command to set a local user account with privilege level and password on the switch.

Command Syntax

username WORD privilege <1-4> password (8 |) LINE

Parameter	Parameter Description	Parameter Value
WORD	User name	-
privilege <1-4>	User privilege level	-
8	Specifies a HIDDEN password will follow	-
LINE	User privilege level	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to add a user with privilege level of 2 and password of 123456:

```
Switch# configure terminal
Switch(config)# username testName privilege 2 password 123456
```

Related Commands

None

2.2.7 re-username newname

Command Purpose

Use this command to reset username.

Command Syntax

re-username WORD newname WORD

Parameter	Parameter Description	Parameter Value
re-username WORD	Old user name	-
newname WORD	New user name	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This is a sample output from this command displaying how to reset username:

```
Switch# configure terminal
Switch(config)# re-username testName newname newname
```

Related Commands

None

2.2.8 cipher detect

Command Purpose

Use this command to set high level of cipher detect.

Command Syntax

cipher detect (strong | normal | none)

Parameter	Parameter Description	Parameter Value
strong	Cipher must contain digital, normal char and special char	-
normal	Cipher must contain digital and normal char	-
none	Disable security check	-

Command Mode

Global Configuration

Default

None

Usage

This cmd will make all un-strong clear text passwords lost

Examples

This is a sample output from this command displaying how to set high level of cipher detect:

```
Switch# configure terminal
Switch(config)# cipher detect strong
```

Related Commands

2.3 FTP Commands

2.3.1 ftp

Command Purpose

To exchange files between local and remote ftp server, use the ftp command in Privileged EXEC mode.

Command Syntax

ftp (mgmt-if |) host

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
HOST	IPv4, IPv6 address or name of the remote host	Support IPv4/IPv6 address or hostname

Command Mode

Privileged EXEC

Default

None

Usage

Use the ftp command to upload and download files from remote ftp server.

Examples

The following example shows how to connect ftp server by ipv4 address:

```
Switch# ftp mgmt-if 10.10.29.160

Connected to 10.10.29.160.
220----- Welcome to Pure-FTPd -----
220-You are user number 1 of 50 allowed.
220-Local time is now 09:00. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.29.160:root): root
331 User root OK. Password required
Password:
230-User root has group access to:  wheel      disk      adm       sys       daemon
230- bin      root
230 OK. Current directory is /root
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

The following example shows how to connect ftp server by ipv6 address:

```
Switch# ftp mgmt-if 2001:1000::2
```

```
Connected to 2001:1000::2 (2001:1000::2).
220 Serv-U FTP Server v10.2 ready...
Name (2001:1000::2:root): Username
331 User name okay, need password.
Password:
230 User logged in, proceed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Related Commands

2.3.2 ftp vrf

Command Purpose

To exchange files between local and remote ftp server in VPN, use the ftp vrf command in Privileged EXEC mode.

Command Syntax

ftp vrf WORD

Parameter	Parameter Description	Parameter Value
WORD	VPN Routing/Forwarding instance name	A string with 1-15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# ftp vrf testvrf
```

Related Commands

None

2.3.3 ftp username

Command Purpose

To create an FTP username, use the ftp username command in Global Configuration. To remove an FTP username, use the no form of this command.

Command Syntax

ftp username USERNAME

no ftp username

Parameter	Parameter Description	Parameter Value
USERNAME	The user name of the remote FTP server	Up to 31 characters

Command Mode

Global Configuration

Default

None

Usage

The username must also follow the rules. They must start with a letter, and have as interior characters only letters, digits, and underline. Names must be 31 characters or fewer.

Examples

The following example creates an FTP username "abc":

```
Switch# configure terminal
Switch(config)# ftp username abc
```

Related Commands

ftp password

ftp passive

2.3.4 ftp password

Command Purpose

To create the password of an FTP username, use the `ftp password` command in Global Configuration. To remove the password of an FTP username, use the `no` form of this command.

Command Syntax

`ftp password ( 8 | ) LINE`

`no ftp password`

Parameter	Parameter Description	Parameter Value
LINE	The password of the user name of the remote FTP server	Up to 128 characters
8	Specifies a hidden password will follow	-

Command Mode

Global Configuration

Default

No `ftp password` is defined.

Usage

The password will be encrypted in running-config if service password-encryption is enabled.

Examples

The following example creates the `ftp password`:

```
Switch# configure terminal
Switch(config)# ftp password abc
```

Related Commands

`ftp username`

`ftp passive`

2.3.5 ftp passive

Command Purpose

To set the FTP mode in passive mode, use the `ftp passive` command in Global Configuration. To restore the configuration to the default, use `no` form of this command.

Command Syntax

`ftp passive`

no ftp passive

Command Mode

Global Configuration

Default

FTP works in Active mode.

Usage

None

Examples

The following example sets the ftp mode to passive:

```
Switch# configure terminal
Switch(config)# ftp passive
```

Related Commands

ftp username

ftp password

2.3.6 show ftp

Command Purpose

To display the ftp configurations, use show ftp command in Privileged EXEC mode.

Command Syntax

show ftp

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example displays the ftp configurations:

```
Switch# show ftp

ftp passive mode: on
ftp username: root
ftp password: unencrypted, abc
Switch#
```

Related Commands

ftp username

ftp password

2.3.7 copy GFILENAME GURLNAME

Command Purpose

Use this command to copy local file to ftp server.

Command Syntax

copy GFILENAME (vrf VRF_NAME |) (mgmt-if | -a SRC_ADDR | -si SRC_INTF) GURLNAME

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf WORD	VPN Routing/Forwarding instance	A string with 1-15 characters
GFILENAME	Copy from local file	The full path and file name, up to 255 characters
GURLNAME	Copy to local file	The full path and file name, up to 255 characters
-a SRC_ADDR	Copy with assigned IP	-
-si SRC_INTF	Copy with assigned Interface	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy local file to ftp server:

```
Switch# copy flash:/test.c tftp://username:password@1.1.1.1:21/running-config
```

Related Commands

None

2.3.8 copy GURLNAME GFILENAME

Command Purpose

Use this command to copy file from ftp server to local.

Command Syntax

```
copy ( vrf VRF_NAME | ) ( mgmt-if | -a SRC_ADDR | -si SRC_INTF ) GURLNAME GFILENAME
```

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf WORD	VPN Routing/Forwarding instance	A string with 1-15 characters
GURLNAME	Copy from URL	The full path and file name, up to 255 characters
GFILENAME	Copy to local file	The full path and file name, up to 255 characters
-a SRC_ADDR	Copy with assigned IP	-
-si SRC_INTF	Copy with assigned Interface	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy file from ftp server to local:

```
Switch# copy ftp://username:password@1.1.1.1:21/test.c flash:test1.c
```

```
get file from ftp://username:password@1.1.1.1:21/test.c
```

```
Received 225 bytes in 0.3 seconds
```

Related Commands

2.4 TFTP Commands

2.4.1 copy GFILENAME GURLNAME

Command Purpose

Use this command to copy local file to tftp server.

Command Syntax

```
copy GFILENAME ( vrf VRF_NAME | ) ( mgmt-if | -a SRC_ADDR | -si SRC_INTF ) GURLNAME
```

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf WORD	VPN Routing/Forwarding instance	A string with 1-15 characters
GFILENAME	Copy from local file	The full path and file name, up to 255 characters
GURLNAME	Copy to local file	The full path and file name, up to 255 characters
-a SRC_ADDR	Copy with assigned IP	-
-si SRC_INTF	Copy with assigned Interface	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy local file to tftp server:

```
Switch# copy flash:/test.c tftp://1.1.1.1/running-config
```

Related Commands

2.4.2 copy GURLNAME GFILENAME

Command Purpose

Use this command to copy file from tftp server to local.

Command Syntax

copy (vrf *VRF_NAME* |) (mgmt-if | -a *SRC_ADDR* | -si *SRC_INTF*) *GURLNAME* *GFILENAME*

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf WORD	VPN Routing/Forwarding instance	A string with 1-15 characters
GURLNAME	Copy from URL	The full path and file name, up to 255 characters
GFILENAME	Copy to local file	The full path and file name, up to 255 characters
-a SRC_ADDR	Copy with assigned IP	-
-si SRC_INTF	Copy with assigned Interface	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy file from tftp server to local:

```
Switch# copy tftp://1.1.1.1/test.c flash:test1.c
```

```
get file from tftp://1.1.1.1/test.c
```

```
.
```

```
Received 225 bytes in 0.3 seconds
```

Related Commands

None

2.4.3 copy running-config mgmt-if

Command Purpose

Use this command to copy running-config to tftp server.

Command Syntax

copy running-config (mgmt-if |) *GURLNAME*

Parameter	Parameter Description	Parameter Value
startup-config	Copy from current system configuration	-
mgmt-if	Management port	-
GURLNAME	Copy to URL	The full path and file name, up to 255 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy running-config to tftp server:

```
Switch#copy running-config tftp://1.1.1.1/running-config
```

```
Building configuration...
```

```
send file to tftp://1.1.1.1/running-config
```

```
...
```

```
Sent 40198 bytes in 8.3 seconds
```

Related Commands

None

2.4.4 copy mgmt-if startup-config

Command Purpose

Use this command to copy startup-config from tftp server.

Command Syntax

Copy (mgmt-if |) *GURLNAME* startup-config

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
GURLNAME	Copy from URL	The full path and file name, up to 255 characters
startup-config	Copy to startup system configuration	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy startup-config from tftp server:

```
Switch#copy tftp://1.1.1.1/startup-config startup-config
```

```
get file from tftp://1.1.1.1/startup-config
```

```
..
```

```
Sent 32252 bytes in 6.4 seconds
```

Related Commands

None

2.5 scp Commands

2.5.1 copy GFILENAME GURLNAME

Command Purpose

Use this command to copy local file to scp server.

Command Syntax

copy *GFILENAME* (*mgmt-if* |) *GURLNAME*

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
GFILENAME	Copy from local file	The full path and file name, up to 255 characters
GURLNAME	Copy to local file	The full path and file name, up to 255 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy local file to scp server:

```
Switch# copy flash:/test.c scp://1.1.1.1/running-config
```

Related Commands

2.5.2 copy *GURLNAME* *GFILENAME*

Command Purpose

Use this command to copy file from scp server to local.

Command Syntax

copy (*mgmt-if* |) *GURLNAME* *GFILENAME*

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
GURLNAME	Copy from URL	The full path and file name, up to 255 characters
GFILENAME	Copy to local file	The full path and file name, up to 255 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy file from scp server to local:

```
Switch# copy scp://1.1.1.1/test.c flash:test1.c
```

```
get file from scp://1.1.1.1/test.c
```

```
.
```

```
Received 225 bytes in 0.3 seconds
```

Related Commands

2.5.3 copy running-config mgmt-if

Command Purpose

Use this command to copy running-config to scp server.

Command Syntax

copy running-config (mgmt-if |) *GURLNAME*

Parameter	Parameter Description	Parameter Value
startup-config	Copy from current system configuration	-
mgmt-if	Management port	-
GURLNAME	Copy to URL	The full path and file name, up to 255 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy running-config to scp server:

```
Switch#copy running-config mgmt-if scp://1.1.1.1/running-config
```

```
Building configuration...
```

```
send file to scp://1.1.1.1/running-config
```

```
...
```

```
Sent 40198 bytes in 8.3 seconds
```

Related Commands

None

2.5.4 copy mgmt-if startup-config

Command Purpose

Use this command to copy startup-config from scp server.

Command Syntax

copy (mgmt-if |) *GURLNAME* startup-config

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
GURLNAME	Copy from URL	The full path and file name, up to 255 characters
startup-config	Copy to startup system configuration	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the command displaying how to copy startup-config from scp server:

```
Switch#copy scp://1.1.1.1/startup-config startup-config

get file from scp://1.1.1.1/startup-config
..
Sent 32252 bytes in 6.4 seconds
```

Related Commands

None

2.6 Telnet Commands

2.6.1 telnet

Command Purpose

Use this command from the switch to access the other devices in the network.

Command Syntax

telnet (*-a SRC_ADDR*) (*vrf WORD* | *mgmt-if*) *HOST* (*PORT* |)

Parameter	Parameter Description	Parameter Value
-a SRC_ADDR	Telnet with assigned IP	-
vrf WORD	VPN Routing/Forwarding instance	A string with 1-15 characters
mgmt-if	Management port	-
HOST	IPv4, IPv6 address or name of the remote host	Support IPv4/IPv6 address or hostname
PORT	TCP Port number	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to Telnet from the switch to a remote host:

```
Switch# telnet mgmt-if 10.10.29.247
```

```
Entering character mode
Escape character is '^J'.
TestOS, Version 2.3(62), fcs
Switch# telnet 2001:1000::1
Entering character mode
Escape character is '^J'.
DUT1#
```

Related Commands

None

2.6.2 ip telnet server source address

Command Purpose

To configure the source address of telnet server on your switch, use the telnet server source address command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

ip telnet server source address (vrf *NAME* |) *IP_ADDR*

no ip telnet server source address

Parameter	Parameter Description	Parameter Value
vrf NAME	Specify a vrf to provide telnet server	A string with 1-15 characters
IP_ADDR	Configure IP address for telnet server working inband	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

You can use this command to modify the address which telnet server works on, and specify a vrf to provide telnet server. The source address can only be 0.0.0.0 or loopback interface's address, 0.0.0.0 indicates that the SSH server address is not specified.

Examples

The following example shows how to specify telnet server source address:

```
Switch# configure terminal
Switch(config)# ip telnet server source address vrf vpn1 10.10.10.1
```

Related Commands

None

2.6.3 ip telnet server source port

Command Purpose

To configure the TCP port for telnet server working inband on your switch, use the telnet server source command in Global Configuration.
To restore the default value, use the no form of this command.

Command Syntax

ip telnet server source port NUMBER

no ip telnet server source port

Parameter	Parameter Description	Parameter Value
port NUMBER	Configure TCP port for telnet server working inband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no telnet server source port" will configure TCP port for telnet server working inband with default value of 23.

Examples

The following example shows how to set the TCP port for telnet server working inband on the switch :

```
Switch# configure terminal
Switch(config)# ip telnet server source port 2323
```

Related Commands

None

2.6.4 ip telnet server source mgmt-if port

Command Purpose

To configure the TCP port for telnet server working outband on your switch, use the `telnet server source` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

`ip telnet server source mgmt-if port NUMBER`

`no ip telnet server source mgmt-if port`

Parameter	Parameter Description	Parameter Value
<code>mgmt-if port NUMBER</code>	Configure TCP port for telnet server working outband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no telnet server sourc mgmt-if port" will configure TCP port for telnet server working outband with default value of 23.

Examples

The following example shows how to set the TCP port for telnet server working outband on the switch :

```
Switch# configure terminal
```

```
Switch(config)# ip telnet server source mgmt-if port 2323
```

Related Commands

None

2.7 SSH Commands

2.7.1 ip ssh server

Command Purpose

To enable SSH service, use `ip ssh server enable` command in Global Configuration. To disable SSH service, use `ip ssh server disable` command.

Command Syntax

`ip ssh server ( enable | disable )`

Parameter	Parameter Description	Parameter Value
enable	Turn on the SSH service	-
disable	Turn off the SSH service	-

Command Mode

Global Configuration

Default

SSH service is enabled.

Usage

None

Examples

The following example enables the SSH service on your switch:

```
Switch# configure terminal
Switch(config)# ip ssh server enable
```

Related Commands

show ip ssh server status

2.7.2 ip ssh server authentication-retries

Command Purpose

To configure Secure Shell (SSH) authentication retry times on your switch, use the `ip ssh server authentication-retries` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

```
ip ssh server authentication-retries COUNT
no ip ssh server authentication-retries
```

Parameter	Parameter Description	Parameter Value
COUNT	The number of retries, with a maximum of 6 authentication retries	1-6

Command Mode

Global Configuration

Default

The default is 6.

Usage

None

Examples

The following examples configure SSH authentication retry times on your switch:

```
Switch# configure terminal
```

```
Switch(config)# ip ssh server authentication-retries 3
```

Related Commands

```
show ip ssh server status
```

2.7.3 ip ssh server authentication-timeout**Command Purpose**

To configure Secure Shell (SSH) authentication timeout on your switch, use the `ip ssh server authentication-timeout` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

```
ip ssh server authentication-timeout SECONDS
```

```
no ip ssh server authentication-timeout
```

Parameter	Parameter Description	Parameter Value
SECONDS	The number of seconds until timeout disconnects	1-120 seconds

Command Mode

Global Configuration

Default

The default is 120 seconds.

Usage

None

Examples

The following examples configure SSH authentication timeout on your switch:

```
Switch# configure terminal
Switch(config)# ip ssh server authentication-timeout 100
```

Related Commands

show ip ssh server status

2.7.4 ip ssh server authentication-type

Command Purpose

To configure Secure Shell (SSH) authentication type on your switch, use the `ip ssh server authentication-type` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

`ip ssh server authentication-type ( all | { password | public-key | rsa } )`

`no ip ssh server authentication-type`

Parameter	Parameter Description	Parameter Value
all	Enable all authentication type	-
password	Enable password authentication	-
public-key	Enable SSHv2 public key authentication	-
rsa	Enable SSHv1 rsa authentication	-

Command Mode

Global Configuration

Default

The default authentication type is `all`.

Usage

None

Examples

The following examples configure SSH authentication type on the switch:

```
Switch# configure terminal
Switch(config)# ip ssh server authentication-type password
```

Related Commands

show ip ssh server status

2.7.5 ip ssh server host-key rsa key

Command Purpose

To configure Secure Shell (SSH) host-key on your switch, use the ip ssh server host-key rsa key command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

```
ip ssh server host-key rsa key KEYNAME
no ip ssh server host-key rsa
```

Parameter	Parameter Description	Parameter Value
KEYNAME	The key value for host key	Up to 32 characters

Command Mode

Global Configuration

Default

None

Usage

Host-key is used to combining public key to generate a session. When SSH login, modifying host-key can cause connection closed.

Examples

The following examples configure SSH host key on your switch:

```
Switch# configure terminal
Switch(config)# ip ssh server host-key rsa key KEY1
```

Related Commands

show ip ssh server status

2.7.6 ip ssh server rekey-interval

Command Purpose

To configure Secure Shell (SSH) rekey interval on your switch, use the `ip ssh server rekey-interval` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

`ip ssh server rekey-interval MINUTE`

`no ip ssh server rekey-interval`

Parameter	Parameter Description	Parameter Value
MINUTE	The rekey interval in minutes	1-1440 minutes

Command Mode

Global Configuration

Default

The default interval is 60 minutes.

Usage

None

Examples

The following examples configure SSH rekey interval on your switch:

```
Switch# configure terminal
```

```
Switch(config)# ip ssh server rekey-interval 30
```

Related Commands

```
show ip ssh server status
```

2.7.7 ip ssh server version

Command Purpose

To configure Secure Shell (SSH) version on your switch, use the `ip ssh server version` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

ip ssh server version (1 | 2 | all)

no ip ssh server version

Parameter	Parameter Description	Parameter Value
1	Switch runs only SSH Version 1	-
2	Switch runs only SSH Version 2	-
all	Version 1 and Version 2 are both supported	-

Command Mode

Global Configuration

Default

The default SSH version is 2.

Usage

You can use this command with the 2 keyword to ensure that your switch will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Switch# configure terminal
Switch(config)# ip ssh server version 1
```

Related Commands

show ip ssh server status

2.7.8 ip ssh server source address

Command Purpose

To configure the source address of Secure Shell (SSH) server on your switch, use the ip ssh server source command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

ip ssh server source address { vrf *NAME* | } *IP_ADDR*

no ip ssh server source address

Parameter	Parameter Description	Parameter Value
vrf <i>NAME</i>	Specify a vrf to provide SSH server	Up to 15 characters
<i>IP_ADDR</i>	Configure IP address for SSH server working inband	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

You can use this command to modify the address which SSH server works on, and specify a vrf to provide SSH server. The source address can only be 0.0.0.0 or loopback interface's address, 0.0.0.0 indicates that the SSH server address is not specified.

Examples

The following example shows how to set SSH server inband address :

```
Switch# configure terminal
Switch(config)# ip ssh server source address 10.10.10.1
```

Related Commands

ip ssh server

2.7.9 ip ssh server source port

Command Purpose

To configure the TCP port for SSH server working inband on your switch, use the ip ssh server source command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

ip ssh server source port *NUMBER*

no ip ssh server source port

Parameter	Parameter Description	Parameter Value
port NUMBER	Configure TCP port for SSH server working inband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no ip ssh server source port" will configure TCP port for SSH server working inband with default value of 22.

Examples

The following example shows the special port is configured:

```
Switch# configure terminal
Switch(config)# ip ssh server source port 2222
```

Related Commands

ip ssh server

2.7.10 ip ssh server source mgmt-if port

Command Purpose

To configure the TCP port for SSH server working outband on your switch, use the ip ssh server source command in Global Configuration.
To restore the default value, use the no form of this command.

Command Syntax

ip ssh server source mgmt-if port *NUMBER*
no ip ssh server source mgmt-if port

Parameter	Parameter Description	Parameter Value
mgmt-if port <i>NUMBER</i>	Configure TCP port for SSH server working outband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no ip ssh server source mgmt-if port" will configure TCP port for SSH server working outband with default value of 22.

Examples

The following example shows the special port is configured:

```
Switch# configure terminal
Switch(config)# ip ssh server source mgmt-if port 2222
```

Related Commands

ip ssh server

2.7.11 show ip ssh server session

Command Purpose

To display the session information for Secure Shell (SSH), use the show ip ssh server session command in Privileged EXEC mode.

Command Syntax

show ip ssh server session

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the current SSH sessions:

```
Switch# show ip ssh server session
```

Version	Encryption	Hmac	User	IP	State
2.0	aes128-cbc	hmac-md5	abc	10.10.29.22	Session started

Related Commands

show ip ssh server status

2.7.12 show ip ssh server status

Command Purpose

To display the version and configuration data for Secure Shell (SSH), use the show ip ssh server status command in Privileged EXEC mode.

Command Syntax

```
show ip ssh server status
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the current SSH configurations:

```
Switch# show ip ssh server status
```

```
SSH server enabled
Version: 1.99
Authentication timeout: 33 second(s)
Authentication retries: 6 time(s)
Server key lifetime: 60 minute(s)
Authentication type: password, public-key
```

Related Commands

```
show ip ssh server session
```

2.7.13 rsa key generate

Command Purpose

To create a key by system, use the rsa key generate command in Global Configuration.

Command Syntax

rsa key KEYNAME generate

Parameter	Parameter Description	Parameter Value
KEYNAME	The name of the key	Up to 32 characters

Command Mode

Global Configuration

Default

None

Usage

Use the rsa key command to create a key by system.

Examples

The following example creates a key named KEY1:

```
Switch# configure terminal
Switch(config)# rsa key KEY1 generate

Generating RSA private key, 1024 bit long modulus
Please waiting for a moment: done!
Public exponent is 65537 (0x10001)
Generate RSA key successfully
Switch(config)#
```

Related Commands

show rsa keys

2.7.14 rsa key

Command Purpose

To create a key, use the rsa key command in Global Configuration.

Command Syntax

rsa key KEYNAME

Parameter	Parameter Description	Parameter Value
KEYNAME	The name of the key	Up to 32 characters

Command Mode

Global Configuration

Default

None

Usage

Use the rsa key command to create a key.

Examples

The following example creates a key named KEY1:

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)#
```

Related Commands

show rsa keys

2.7.15 key format

Command Purpose

To specify the key format, use the key format command in RSA key configuration mode.

Command Syntax

key format (der | pem)

Parameter	Parameter Description	Parameter Value
der	The format is der	-
pem	The format is pem	-

Command Mode

Rsa Key Configuration

Default

The default key format is DER.

Usage

None

Examples

The following example specify the key format of KEY1 as der :

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# key format der
```

Related Commands

rsa key

2.7.16 key string end

Command Purpose

To exit the rsa key configuration mode to Global Configuration and apply all rsa key configurations, use the key string end command in RSA key configuration mode.

Command Syntax

key string end

Command Mode

Rsa Key Configuration

Default

None

Usage

None

Examples

The following example shows exit the rsa key configuration mode :

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# key string end
Switch(config)#
```

Related Commands

rsa key

2.7.17 key type

Command Purpose

To specify the key type, use the key type command in RSA key configuration mode.

Command Syntax

key type (public | private)

Parameter	Parameter Description	Parameter Value
public	Specify the key as a public key	-
private	Specify the key as a private key	-

Command Mode

Rsa Key Configuration

Default

None

Usage

None

Examples

The following example specifies the key type of KEY1 as public key:

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# key type public
```

Related Commands

rsa key

2.7.18 reset

Command Purpose

To clear all key configurations, use the reset command in RSA key configuration mode.

Command Syntax

```
reset
```

Command Mode

Rsa Key Configuration

Default

None

Usage

None

Examples

The following example shows to clear all configurations for the key KEY1:

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# reset
```

Related Commands

rsa key

2.7.19 validate

Command Purpose

To check the validation of the key strings, use the validate command in RSA key configuration mode.

Command Syntax

```
validate
```

Command Mode

Rsa Key Configuration

Default

None

Usage

None

Examples

The following example shows to validate key strings of the key KEY1:

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# validate
```

Related Commands

rsa key

2.7.20 KEYLINE**Command Purpose**

To add key strings from the screen directly, type any strings in RSA key configuration mode except the keywords in this mode.

Command Syntax

KEYLINE

Parameter	Parameter Description	Parameter Value
KEYLINE	key line	key line string

Command Mode

Rsa Key Configuration

Default

None

Usage

Type any key string.

Examples

The following example shows to type a key string of the key KEY1:

```
Switch# configure terminal
Switch(config)# rsa key KEY1
Switch(config-rsa-key)# 00302017 4A7D385B 1234EF29 335FC973
Switch(config-rsa-key)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
```

Related Commands

Validate

2.7.21 rsa key export

Command Purpose

To export the key file to a specified destination, use the rsa key export command in Global Configuration.

Command Syntax

rsa key *KEYNAME* export url *DEST_FILE* (public | private) (der | der-hex | pem | ssh1 | ssh2)

Parameter	Parameter Description	Parameter Value
KEYNAME	Specify the key name to display	Up to 32 characters
DEST_FILE	The destination file path and name	The full path and file name, up to 255 characters
public	Specify the key as a public key	-
private	Specify the key as a private key	-
der	DER format	-
der-hex	DER HEX format	-
pem	PEM format	-
ssh1	SSHv1 format	-
ssh2	Specify the key format	-

Command Mode

Global Configuration

Default

None

Usage

Use the rsa key generate command to generate a key.

Examples

The following example shows to export the key KEY1 to flash as a public key:

```
Switch# configure terminal
```

```
Switch(config)# rsa key KEY1 export url flash:/key1.pub public ssh2
```

The following example shows to export the key KEY2 to flash as a private key:

```
Switch# configure terminal
```

```
Switch(config)# rsa key KEY2 export url flash:/key1 private ssh1
```

Related Commands

rsa key generate

rsa key import

2.7.22 rsa key import

Command Purpose

To import the key file from a specified source, use the `rsa key import` command in Global Configuration.

Command Syntax

```
rsa key KEYNAME import url SRC_FILE ( public | private ) ( der | der-hex | pem | ssh1 | ssh2 )
```

Parameter	Parameter Description	Parameter Value
KEYNAME	Specify the key name to display	Up to 32 characters
SRC_FILE	The destination file path and name	The full path and file name, up to 255 characters
public	Specify the key as a public key	-
private	Specify the key as a private key	-
der	DER format	-
der-hex	DER HEX format	-
pem	PEM format	-
ssh1	SSHv1 format	-
ssh2	Specify the key format	-

Command Mode

Global Configuration

Default

None

Usage

Use the `rsa key` to generate command to generate a key.

Examples

The following example shows to import the key KEY1 to flash as a public key:

```
Switch# configure terminal
```

```
Switch(config)# rsa key KEY1 import url flash:/key1.pub public ssh2
```

The following example shows to import the key KEY2 to flash as a private key:

```
Switch# configure terminal
```

```
Switch(config)# rsa key KEY2 import url flash:/key1 private ssh1
```

Related Commands

rsa key generate

rsa key export

2.7.23 show rsa key

Command Purpose

To display the details of the keys, use the show rsa key command in Privileged EXEC mode.

Command Syntax

show rsa key *KEYNAME*

Parameter	Parameter Description	Parameter Value
KEYNAME	Specify the key name to display	Up to 32 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example displays the detailed information of the key named "KEY1":

```
Switch# show rsa key KEY1
```

RSA key information:

```
=====
```

```

Name: KEY1
Type: private
Modulus: 1024 bit
Usage count: 0
Private key DER code:
30820258
    0201
        00
    028180
        9B3E9726 6405BD54 692F172A901F3879 C947366E 5703D282 AA31707F 214D38C9

```

Related Commands

show rsa keys

2.7.24 show rsa keys

Command Purpose

To display the brief information of all the keys, use the show rsa keys command in Privileged EXEC mode.

Command Syntax

show rsa keys

Command Mode

Privileged EXEC

Default

None

Usage

Use the rsa key generate command to generate a key.

Examples

The following example displays the brief information of the keys:

```
Switch# show rsa keys
```

Name	Type	Usage	Modulus
=====			

key1	private	0	1024
key2	public	0	1024

Related Commands

show rsa key

2.7.25 ssh

Command Purpose

To connect to the remote SSH server, use the ssh command in Privileged EXEC mode.

Command Syntax

ssh -l NAME ({ -i KEYNAME | -p DPORT | -v (1 | 2) | -c { 3des | des | 3des-cbc | aes128-cbc | aes192-cbc | aes256-cbc } | -m { hmac-md5-128 | hmac-md5-96 | hmac-sha1-160 | hmac-sha1-96 } | -o numberofpasswordprompts NUM | -a A.B.C.D } |) (mgmt-if |) (A.B.C.D | X:X::X:X | HOST)

Parameter	Parameter Description	Parameter Value
-l NAME	Log in using this user name	Up to 31 characters
-i KEYNAME	Specify the name of RSA private key	Up to 32 characters
-p DPORT	Specify the remote port	1-65535
-v (1 2)	Specify SSH protocol version	-
-c	Select encryption algorithm	-
3des	Triple DES (SSHv1 only)	-
des	DES (SSHv1 only)	-
3des-cbc	Triple DES (SSHv2 only)	-
aes128-cbc	AES 128 bits (SSHv2 only)	-
aes192-cbc	AES 192 bits (SSHv2 only)	-
aes256-cbc	AES 256 bits (SSHv2 only)	-
-m	Select HMAC algorithm	-
hmac-md5-128	MD5 based HMAC (128 bits, SSHv2 only)	-
hmac-md5-96	MD5 based HMAC (96 bits, SSHv2 only)	-
hmac-sha1-160	SHA1 based HMAC (160 bits, SSHv2 only)	-
hmac-sha1-96	SHA1 based HMAC (96 bits, SSHv2 only)	-
-o numberofpasswordprompts NUM	Specify number of password prompts with	The range in [1, 7]
-a A.B.C.D	Ssh with assigned IP	IPv4 Address
mgmt-if	Use Management port	-
A.B.C.D	Specify IP address of remote system	IPv4 Address
X:X::X:X	Specify IPv6 address of remote system	IPv6 Address
HOST	Specify hostname of remote system	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example displays the usage of this command:

```
Switch# ssh -l aaa -v 2 1.1.1.1
```

```
aaa@1.1.1.1's password:
```

```
Switch#
```

Related Commands

ip ssh server

2.8 Time&Timezone Commands

2.8.1 clock set datetime

Command Purpose

Use this command to set system current date and time on the Switch.

Command Syntax

clock set datetime *HH:MM:SS MONTH DAY YEAR*

Parameter	Parameter Description	Parameter Value
HH:MM:SS	Specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone	HH:MM:SS in 24-hour format.
MONTH	Specify the month by name	Should be in range 1 to 12
DAY	Specify the day by date in the month	Should be in range 1 to 31
YEAR	Specify the year	Should be in range 1993 to 2035

Command Mode

Global Configuration

Default

The default time is based from UTC.

Usage

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

Examples

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2014:

```
Switch# configure terminal
Switch(config)# clock set 13:32:00 23 7 2014
```

Related Commands

show clock

2.8.2 clock set timezone

Command Purpose

Use this command to set the time zone on the Switch.

To restore to the default time of UTC, use the no form of this command.

Command Syntax

clock set timezone ZONE (add | minus) hours-offset [minutes-offset] [seconds-offset]

no clock set timezone

Parameter	Parameter Description	Parameter Value
ZONE	Specify the zone name	the length should be [3, 32], and only [a-zA-Z_] is supported, and the first and last character must be alphabet.
add	Specify the time offset is positive from UTC	-
minus	Specify the time offset is negative from UTC	-
HOUR_OFFSET	Specify the time offset in hours	0-23
MINUTES_OFFSET	[optional]Specify the time offset in minutes, should be in range 0 to 59	0-59
SECONDS_OFFSET	[optional]Specify the time offset in seconds	0-59

Command Mode

Global Configuration

Default

The default time zone should be UTC.

Usage

None

Examples

The following example sets the Atlantic Canada time zone is 3.5 hours less than UTC:

```
Switch# configure terminal
```

```
Switch(config)# clock set timezone Canada minus 3 30
```

The following example sets the time zone named ZZZ is 5 hours faster than UTC:

```
Switch# configure terminal
```

```
Switch(config)# clock set timezone ZZZ add 5
```

Related Commands

show clock (detail)

2.8.3 clock set summer-time

Command Purpose

Use this command to set summer time (daylight saving time) in areas where it starts and ends on a particular day each year(recurring) or on specified year(date).

To restore to the default time of UTC, use the no form of this command.

Command Syntax

clock set summer-time ZONE recurring start-time end-time offset

clock set summer-time ZONE date start-time end-time offset

no clock set summer-time

Parameter	Parameter Description	Parameter Value
ZONE	Specify the summer zone name	The length should be [3, 32), and only [a-zA-Z_] is supported, and the first and last character must be alphabet.
recurring	Specify that summer time starts and ends on a particular day of the week each year	-
date	Specify that summer time starts and ends on a particular day of the specified year	-

Parameter	Parameter Description	Parameter Value
START_TIME	Specify the start time of summer time	For recurring summer time, the format should be month, day, hh:mm:ss or (first second third fourth last) DAY <1-12> HH:MM:SS, while for date summer time, the format should be month, day, year, hh:mm:ss
END_TIME	Specify the end time of summer time	For recurring summer time, the format should be month, day, hh:mm:ss or (first second third fourth last) DAY <1-12> HH:MM:SS, while for date summer time, the format should be month, day, year, hh:mm:ss
OFFSET	For offset, specify the number of minutes to add during summer time. The default is 60.	1-1440 minutes

Command Mode

Global Configuration

Default

Summer time should be disabled by default.

Usage

The first part of the clock summer-time global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

Examples

This example shows how to specify that summer time starts on June 1st at 0200 and ends on the October 31 at 0200:

```
Switch# configure terminal
```

```
Switch(config)# clock set summer-time stime recurring 6 1 02:00:00 10 31 02:00:00 120
```

This example shows how to specify that summer time starts on March the second Wednesday at 0200 and ends on the August the last Friday at 0100:

```
Switch# configure terminal
```

```
Switch(config)# clock set summer-time stime recurring second Wed 3 02:0:0 last Fri 8 01:0:0 60
```

Related Commands

show clock (detail)

2.8.4 show clock

Command Purpose

Use this command to display the current time and date configuration.

Command Syntax

show clock (detail |)

Parameter	Parameter Description	Parameter Value
detail	Display the configured timezone and summer time information in addition to current date and time	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays current time and date in detail:

```
Switch#show clock detail
```

```
10:43:00 beijing Fri Oct 25 2013
```

```
Time zone: (GMT + 08:00:00) beijing
```

Related Commands

show clock

2.8.5 show timezones

Command Purpose

Use this command to display all the timezones in world.

Command Syntax

show timezons

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays all the current timezones:

```
Switch#show timezones
```

```
(GMT+00:06:04)   Europe/Andorra
(GMT+03:41:12)   Asia/Dubai
(GMT+04:36:48)   Asia/Kabul
(GMT-04:07:12)   America/Antigua
(GMT-04:12:16)   America/Anguilla
(GMT+01:19:20)   Europe/Tirane
(GMT+02:58:00)   Asia/Yerevan
(GMT-04:36:00)   America/Curacao
(GMT+00:52:56)   Africa/Luanda
(GMT+11:06:24)   Antarctica/McMurdo    McMurdo Station, Ross Island
=====
(GMT+00:00:00)   Antarctica/South_Pole Amundsen-Scott Station, South Pole
(GMT-04:32:32)   Antarctica/Rothera    Rothera Station, Adelaide Island
(GMT-04:16:24)   Antarctica/Palmer     Palmer Station, Anvers Island
```

Related Commands

show clock

2.9 HTTP commands Commands

2.9.1 service http

Command Purpose

To enable HTTP service, use service http enable command in Global Configuration. To disable HTTP service, use service http disable command.

Command Syntax

service http (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Turn on the HTTP service	-
disable	Turn off the HTTP service	-

Command Mode

Global Configuration

Default

HTTP service is disabled.

Usage

The WEB image should be loaded first.

Examples

The following example shows how to enable HTTP service:

```
Switch# configure terminal
Switch(config)# service http enable
```

Related Commands

http server load

http timeout

2.9.2 service https

Command Purpose

To enable HTTPS service, use service http enable command in Global Configuration. To disable HTTPS service, use service http disable command.

Command Syntax

service https (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Turn on the HTTPS service	-
disable	Turn off the HTTPS service	-

Command Mode

Global Configuration

Default

HTTPS service is disabled.

Usage

The WEB image should be loaded first.

Examples

The following example shows how to enable HTTPS service:

```
Switch# configure terminal
Switch(config)# service https enable
```

Related Commands

http server load

http timeout

2.9.3 http server load

Command Purpose

To load WEB image, user the http server load command .

Command Syntax

http server load FILENAME

Parameter	Parameter Description	Parameter Value
FILENAME	Name of WEB image	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to specify web image:

```
Switch# configure terminal
Switch(config)# http server load flash:/webImage.bin
```

Related Commands

service http enable
service https enable
http timeout

2.9.4 http timeout

Command Purpose

To configure the expire time of online web users.

Command Syntax

http timeout TIMEOUT

Parameter	Parameter Description	Parameter Value
TIMEOUT	Online web user expire time	The range is [1,60], unit is minute

Command Mode

Global Configuration

Default

20min.

Usage

None

Examples

The following example shows how to configure http timeout:

```
Switch# configure terminal
Switch(config)# http timeout 30
```

Related Commands

http server load
service http enable
service https enable

2.9.5 http server source address

Command Purpose

To configure the source address of WEB server on your switch, use the http server source address command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

http server source address (vrf *NAME* |) *A.B.C.D*
no http server source address

Parameter	Parameter Description	Parameter Value
vrf <i>NAME</i>	Specify a vrf to provide WEB server	A string with 1-15 characters
<i>A.B.C.D</i>	Configure IP address for WEB server working	-

Command Mode

Global Configuration

Default

None

Usage

You can use this command to modify the address which WEB server works on, and specify a vrf to provide WEB server. The source address can only be 0.0.0.0 or loopback interface's address, 0.0.0.0 indicates that the WEB server address is not specified.

Examples

The following example shows how to set inband http server address:

```
Switch# configure terminal
Switch(config)# http server source address 10.10.10.1
```

Related Commands

http server load
service http enable
service https enable

2.9.6 http server source port

Command Purpose

To configure the TCP port for HTTP server working inband on your switch, use the `http server source port` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

`http server source port` *PORT*

`no http server source port`

Parameter	Parameter Description	Parameter Value
PORT	Configure TCP port for HTTP server working inband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no http server source port" will configure TCP port for HTTP server working inband with default value of 80.

Examples

The following example shows how to set inband http server TCP port:

```
Switch# configure terminal
Switch(config)# http server source port 1080
```

Related Commands

`http server load`
`service http enable`
`service https enable`

2.9.7 http server source ssl-port

Command Purpose

To configure the TCP port for HTTPS server working inband on your switch, use the `http server source ssl-port` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

`http server source ssl-port PORT`

`no http server source ssl-port`

Parameter	Parameter Description	Parameter Value
PORT	Configure TCP port for HTTPS server working inband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no http server source ssl-port" will configure TCP port for HTTPS server working inband with default value of 443.

Examples

The following example shows how to set inband https server TCP port:

```
Switch# configure terminal
```

```
Switch(config)# http server source port 10443
```

```
Switch# configure terminal
```

```
Switch(config)# http server source ssl-port 10443
```

Related Commands

`http server load`

`service http enable`

`service https enable`

2.9.8 http server source mgmt-if port

Command Purpose

To configure the TCP port for HTTP server working outband on your switch, use the `http server source mgmt-if port` command in Global Configuration. To restore the default value, use the `no` form of this command.

Command Syntax

http server source mgmt-if port *PORT*

no http server source mgmt-if port

Parameter	Parameter Description	Parameter Value
<i>PORT</i>	Configure TCP port for HTTP server working outband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no http server source mgmt-if port" will configure TCP port for HTTP server working outband with default value of 80.

Examples

The following example shows how to set outband http server TCP port:

```
Switch# configure terminal
```

```
Switch(config)# http server source mgmt-if port 1080
```

Related Commands

http server load

service http enable

service https enable

2.9.9 http server source mgmt-if ssl-port

Command Purpose

To configure the TCP port for HTTPS server working outband on your switch, use the http server source mgmt-if ssl-port command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

http server source mgmt-if ssl-port *PORT*

no http server source mgmt-if port

Parameter	Parameter Description	Parameter Value
<i>PORT</i>	Configure TCP port for HTTPS server working outband	1025-65535

Command Mode

Global Configuration

Default

None

Usage

The CLI of "no http server source mgmt-if ssl-port" will configure TCP port for HTTPS server working outband with default value of 443.

Examples

The following example shows how to set outband https server TCP port:

```
Switch# configure terminal
```

```
Switch(config)# http server source port 10443
```

Related Commands

http server load

service http enable

service https enable

2.9.10 http authentication aaa

Command Purpose

To configure the AAA method list for web login on your switch, use the http authentication aaa command in Global Configuration. To restore the default value, use the no form of this command.

Command Syntax

http authentication (local | aaa (login-authentication | exec-authorization) (default | LISTNAME))

no http authentication (aaa (login-authentication | exec-authorization))

Parameter	Parameter Description	Parameter Value
local	Configure web login authentication by local	-
aaa	Configure web login authentication by AAA	-
login-authentication	Configure web login authentication method list	-
exec-authorization	Configure web login authorization method list	-
default	Set method list name default	-
LISTNAME	Set method list name	Up to 31 characters

Command Mode

Global Configuration

Default

default web login method is local

Usage

The CLI of "http authentication (local |aaa (login-authentication|exec-authorization) (default|LISTNAME))" can only be configured when AAA is enable.

Examples

The following example shows how to set web AAA login method to be default.:

```
Switch# configure terminal
```

```
Switch(config)# http authentication aaa login-authentication default
```

Related Commands

aaa new-model

aaa authentication login

aaa authorization exec

2.10 RPC-API commands Commands

2.10.1 service rpc-api

Command Purpose

To enable RPC-API service, use service rpc-api enable command in Global Configuration. To disable RPC-API service, use service rpc-api disable command.

Command Syntax

```
service rpc-api ( enable ( port PORT | ssl ( ssl-port SSLPORT | ) ) ( vrf NAME | ) | disable )
```

```
service rpc-api disable
```

Parameter	Parameter Description	Parameter Value
enable	Turn on the RPC-API service	-
disable	Turn off the RPC-API service	-
PORT	TCP port number. TCP port number. By default, the RPC-API service listens on TCP port 80 (HTTP)	1025-65535

Parameter	Parameter Description	Parameter Value
vrf NAME	VPN Routing/Forwarding instance	A string with 1-15 characters
ssl	Enable SSL (HTTPS)	-
SSLPORT	TCP port number. TCP port number. By default, the RPC-API service listens on TCP port 443 (HTTPS)	1025-65535

Command Mode

Global Configuration

Default

Disabled.

Usage

None

Examples

The following example shows how to enable RPC-API service:

```
Switch# configure terminal
Switch(config)# service rpc-api enable port 2000
```

Related Commands

```
show services rpc-api
service rpc-api auth-mode
```

2.10.2 service rpc-api auth-mode

Command Purpose

To enable RPC-API HTTP Basic authentication.

Command Syntax

```
service rpc-api auth-mode basic
no service rpc-api auth-mode
```

Command Mode

Global Configuration

Default

Disabled.

Usage

Once enable or disable RPC-API HTTP Basic authentication, and users want to continue to use RPC-API service, users must re-enable it.

Examples

The following example shows how to enable RPC-API HTTP Basic authentication:

```
Switch# configure terminal
Switch(config)# service rpc-api auth-mode basic
```

Related Commands

service rpc-api enable
show services rpc-api

2.10.3 show services rpc-api**Command Purpose**

To show RPC-API configuration information.

Command Syntax

```
show services rpc-api
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the configuration information:

```
Switch(config)# show services rpc-api
```

RPC API services configuration:

HTTP server: shutdown, port: 80, authentication mode: none

Related Commands

service rpc-api enable

Chapter 3 Ethernet Commands

3.1 Interface Commands

3.1.1 Bandwidth

Command Purpose

Use this command to set the bandwidth of the port.

To return the bandwidth to default value, use the no form of this command.

Command Syntax

bandwidth BANDWIDTH

no bandwidth

Parameter	Parameter Description	Parameter Value
BANDWIDTH	port bandwidth	1-100000000, unit: kbps

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example set the bandwidth of the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# bandwidth 1000
```

The following example returns the bandwidth to default value:

```
Switch# configure terminal
Switch(config-if)# no bandwidth
```

Related Commands

duplex

Speed

3.1.2 clear counters

Command Purpose

Use this command to clear the counters on the physical interface.

Command Syntax

clear counters (IFNAME |)

Parameter	Parameter Description	Parameter Value
IFNAME	Only clear the specified interface statistics	Support physical/aggregation ports

Command Mode

Privileged EXEC

Default

None

Usage

The clear counters command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.

Examples

The following example clears the counters on all interfaces:

```
Switch# clear counters
```

The following example clears the counters on the interface eth-0-1:

```
Switch# clear counters eth-0-1
```

The following example clears the counters on the agg1:

```
Switch# clear counters agg1
```

Related Commands

None

3.1.3 Description

Command Purpose

Use this command to set the description on the interface.

To remove the description on the interface, use the no form of this command.

Command Syntax

description LINE

no description

Parameter	Parameter Description	Parameter Value
LINE	The description on the interface	should be no more than 240 characters, and the character can not include '?'

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example sets the description on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# description Ethernet
```

The following example removes the description on the interface:

```
Switch# configure terminal
Switch(config-if)# no description
```

Related Commands

None

3.1.4 Duplex

Command Purpose

Use the duplex interface configuration command to specify the duplex mode of operation for a port. Use the no form of this command to return the port to its default value.

Command Syntax

duplex (auto | full | half)

no duplex

Parameter	Parameter Description	Parameter Value
auto	Enable automatic duplex configuration; port automatically detects whether it should run in full-duplex or half-duplex mode, depending on the attached device mode	-
full	Enable full-duplex mode	-
half	Enable half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You can not configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s	-

Command Mode

Interface Configuration

Default

auto

Usage

The command is not allowed to be set on 10G port or optical mode of combo port.

Examples

The following example sets the duplex mode to auto:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# duplex auto
```

The following example sets the duplex mode to full:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# duplex full
```

The following example returns the duplex mode to default:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no duplex
```

Related Commands

bandwidth

Speed

3.1.5 Speed

Command Purpose

Use the speed interface configuration command to specify the speed of port. Use the no of this command to return the port to its default value.

Command Syntax

speed (10 | 100 | 1000 | 2G5 | 5G | 10G | 40G | 100G | auto)

no speed

Parameter	Parameter Description	Parameter Value
auto	Port automatically detects the speed it should run	-
10	Port runs at 10 Mb/s	-

Parameter	Parameter Description	Parameter Value
100	Port runs at 100 Mb/s	-
1000	Port runs at 1000 Mb/s	-
2G5	Port runs at 2.5Gb/s	-
5G	Port runs at 5Gb/s	-
10G	Port runs at 10Gb/s	-
40G	Port runs at 40Gb/s	-
100G	Port runs at 100Gb/s	-

Command Mode

Interface Configuration

Default

auto

Usage

The command is not allowed to be set on optical mode of combo port.

Examples

This example shows how to set the speed on a port to 1000 Mb/s:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# speed 1000
```

This example shows how to return the speed on a port to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no speed
```

Related Commands

bandwidth

Duplex

3.1.6 Interface

Command Purpose

Use this command to enter interface mode.

Command Syntax

interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	The name of interface, i.e. eth-0-1, agg1, vlan1, loopback1	Support all interface types

Command Mode

Global Configuration

Default

None

Usage

The interface name can be either a port name (i.e. eth-0-1) or link-agg name (i.e. agg1) or vlan name (i.e. vlan2) or loop-back name (i.e. loopback10).

Examples

The following example enters the interface mode for eth-0-1:

```
Switch(config)# interface eth-0-1
```

The following example enters the interface mode for agg1:

```
Switch(config)# interface agg1
```

The following example enters the interface mode for vlan2:

```
Switch(config)# interface vlan2
```

Related Commands

Exit

3.1.7 interface range

Command Purpose

Use this command to operate a list of interfaces, the interface include physical port, vlan interface, linkagg interface and loopback interface.

Command Syntax

interface range IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	Interface range	Support all interface types can be separate by comma, dash

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example operate a list of physical interface:

```
Switch(config)# interface range eth-0-1 – 24
Switch(config-if-range)# shutdown
```

The following example operate a list of vlan interface:

```
Switch(config)# interface range vlan 1 - 20
Switch(config-if-range)# shutdown
```

The following example operate a list of linkagg interface:

```
Switch(config)# interface range agg 10 - 20
Switch(config-if-range)# shutdown
```

The following example operate a list of loopback interface:

```
Switch(config)# interface range loopback 0 - 5
Switch(config-if-range)# shutdown
```

Related Commands

None

3.1.8 interface range create vlan

Command Purpose

Use this command to create a list of vlan interface.

Command Syntax

interface range create vlan VLAN_RANGE

Parameter	Parameter Description	Parameter Value
VLAN_RANGE	VLAN ID range	VLAN ID range is 1-4094, can be separate by comma, dash

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example create vlan interface 10 to 20:

```
Switch(config)# interface range create vlan 10 - 20
Switch(config-if-range)# shutdown
```

Related Commands

None

3.1.9 Jumboframe

Command Purpose

Use this command to enable jumbo frame. To disable jumbo frame, use the no form of this command.

Command Syntax

jumboframe enable

no jumboframe enable

Command Mode

Interface Configuration

Default

None

Usage

Jumboframe is disabled by default. The max frame which can be transmitted is 1534 bytes. When enable jumboframe, the max frame can be 9600 bytes.

Examples

The following example enables the jumboframe:

```
Switch(config)# interface eth-0-1
Switch(config-if)# jumboframe enable
```

The following example disables the jumboframe:

```
Switch(config-if)# no jumboframe enable
```

Related Commands

None

3.1.10 media-type

Command Purpose

Use the media-type interface configuration command to select a media type for an interface. Use the no form of this command restore to the default value.

Command Syntax

media-type (auto-select | rj45 | sfp)

Parameter	Parameter Description	Parameter Value
auto-select	Enable the switch to dynamically select the type based on which one first links up	-
rj45	Select the RJ-45 interface	-
sfp	Select the small form-factor pluggable (SFP) module interface	-

Command Mode

Interface Configuration

Default

Auto-select

Usage

By default, we use auto-select mode.

Examples

The following example shows how to configure the interface as a rj45 media:

```
Switch(config)# interface eth-0-1
Switch(config-if)# media-type rj45
```

The following example shows how to restore to default value:

```
Switch(config-if)# no media-type
```

Related Commands

None

3.1.11 Unidirectional

Command Purpose

Use the unidirectional interface configuration command to enable/disable unidirectional function.

Command Syntax

unidirectional (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	enable unidirectional function	-
disable	disable unidirectional function	-

Command Mode

Interface Configuration

Default

disable unidirectional function

Usage

Enable unidirectional function will force enable the interface TX function and force disable the interface RX function.

Only fiber port support the unidirectional function, and in 1000M speed mode, duplex must be forced to full mode.

Examples

The following example shows how to enable unidirectional function:

```
Switch(config)# interface eth-0-1
Switch(config-if)# unidirectional enable
```

The following example shows how to disable unidirectional function:

```
NoneSwitch(config-if)# unidirectional disable
```

Related Commands

3.1.12 shutdown

Command Purpose

Use the shutdown interface configuration command to admin down an interface. Use the no form of this command to admin up an interface.

Command Syntax

shutdown

no shutdown

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to shutdown a port:

```
Switch(config)# interface eth-0-1
Switch(config-if)# shutdown
```

The following example shows how to admin up a port:

```
Switch(config-if)# no shutdown
```

Related Commands

None

3.1.13 split interface

Command Purpose

Use the command to split physic port to 10G port. Use the no form of this command to un-split the physic port.

Command Syntax

split interface IFNAME (10giga | 40giga)

no split interface

Parameter	Parameter Description	Parameter Value
IFNAME	the physic port need to split	Support physical ports
10giga	split physic port to four 10G port	-
40giga	split physic port to one 10G port	-

Command Mode

Global Configuration

Default

None

Usage

Need save configuration and reboot to make command take effect

Examples

The following example shows how to split interface to four 10G port:

```
Switch# configure terminal
Switch(config)# split interface eth-0-1 10giga
```

Related Commands

None

3.1.14 load-interval

Command Purpose

Use the load-interval interface configuration command to specify the interval when calculating speed of an interface. Use the no of this command to return the port to its default value.

Command Syntax

load-interval SECONDS

no load-interval

Parameter	Parameter Description	Parameter Value
SECONDS	Load interval	30-600, unit:second

Command Mode

Interface Configuration

Default

300 seconds

Usage

Load-interval must be in increments of 30 second and its default value is 300 second.

Examples

This example shows how to set the load-interval on a port to 600 second:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# load-interval 600
```

This example shows how to return the load-interval on a port to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no load-interval
```

Related Commands

show interface

3.1.15 vlan dot1q tag native

Command Purpose

Use the vlan dot1q tag native global configuration command to configure the edge switch so that all packets going out an 802.1Q trunk, including the native VLAN.

Command Syntax

vlan dot1q tag native

no vlan dot1q tag native

Command Mode

Interface Configuration

Default

None

Usage

Use this command to enable tagging native. If enabled, the packet in native vlan will be tagged with the native vlan. Otherwise, it will be untagged.

Examples

This example shows how to tag native for trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no vlan dot1q tag native
```

This example shows how to disable tagging native for trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no vlan dot1q tag native
```

Related Commands

None

3.1.16 show interface

Command Purpose

Use this command to display the configurations and statistics on all interfaces or an interface.

Command Syntax

show interface (IFNAME |)

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	eth:Physical interface agg:Aggregation interface loopback: Loopback interface vlan:Vlan interface tunnel:Tunnel interface null:Null interface

Command Mode

Privileged EXEC

Default

None

Usage

The OAM statistics can only display when port is 10G mode.

Examples

This example shows how to display the configurations and statistics on the interface eth-0-1:

```
Switch# show interface eth-0-1

Interface eth-0-1
  Interface current state: UP
  Hardware is Ethernet, address is 001e.080a.5102 (bia 001e.080a.5102)
  Bandwidth 1000000 kbits
  Index 1 , Metric 1 , Encapsulation ARPA
  Speed - 1000Mb/s , Duplex - Full , Media type is 1000BASE_T_SFP
  Link type is autonegotiation
  Admin input flow-control is off, output flow-control is off
  Oper input flow-control is off, output flow-control is off
  The Maximum Frame Size is 1632 bytes
  VRF binding: not bound
  ARP timeout 01:00:00, ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is disabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 unicast, 0 broadcast, 0 multicast
    0 runs, 0 giants, 0 input errors, 0 CRC
    0 frame, 0 overrun, 0 pause input
    24 packets output, 2160 bytes
    Transmitted 0 unicast, 24 broadcast, 0 multicast
    0 underruns, 0 output errors, 0 pause output
```

Related Commands

show interface status

3.1.17 show interface status

Command Purpose

Use this command to display the brief information on all Ethernet and link aggregation interfaces.

Command Syntax

show interface (IFNAME |) status

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support aggregation and physical ports

Command Mode

Privileged EXEC

Default

None

Usage

This command will not show VLAN and tunnel interfaces' information.

Examples

This example shows how to display the brief information on all Ethernet and LAG interfaces:

Switch# show interface status

Port	Status	Duplex	Speed	Mode	Type	Description
eth-0-1	down	a-full	a-1000	ACCESS	1000BASE_T	
eth-0-2	down	a-full	a-1000	ACCESS	1000BASE_T	
eth-0-3	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-4	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-5	up	a-full	a-1000	routed	1000BASE_T	
eth-0-6	up	a-full	a-100	ACCESS	1000BASE_T	
eth-0-7	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-8	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-9	down	a-full	a-1000	ACCESS	1000BASE_T	
eth-0-10	down	a-full	a-1000	ACCESS	1000BASE_T	
eth-0-11	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-12	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-13	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-14	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-15	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-16	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-17	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-18	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-19	admin down	auto	auto	ACCESS	1000BASE_T	
eth-0-20	admin down	auto	auto	ACCESS	1000BASE_T	

Related Commands

None

3.1.18 show interface summary**Command Purpose**

Use this command to display the summary on all interfaces or an interface.

Command Syntax

show interface (IFNAME |) summary

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support all interface types

Command Mode

Privileged EXEC

Default

None

Usage

This command will display the summary on all interfaces or an interface in the form of list.

Examples

This example shows how to display the summary on the interface eth-0-1:

```
Switch# show interface eth-0-1 summary
```

```

RXBS: rx rate (bits/sec)      RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)      TXPS: tx rate (pkts/sec)

Interface  Link  RXBS      RXPS      TXBS      TXPS
-----
eth-0-1    DOWN  0          0          0          0

```

Related Commands

show interface

3.1.19 show ip interface**Command Purpose**

Use this command to show layer3 interface information.

Command Syntax

```
show ip interface ( IFNAME | )
```

```
show ip interface brief
```

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name, can be eth, vlan or agg	Support all interface types

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the vlan interface information:

```
Switch# show interface vlan10
```

```

Interface vlan10
  Interface current state: DOWN
  Hardware is VLAN, address is 8633.d260.6500 (bia 8633.d260.6500)
  Bandwidth 1000000 kbits
  Index 4098 , Metric 1 , Encapsulation ARPA
  The maximum transmit unit (MTU) is 1500 bytes
  VRF binding: not bound
  Label switching is disabled
  No virtual circuit configured

```

```
VRRP master of: VRRP is not configured on this interface
ARP timeout 01:00:00, ARP retry interval 1s
```

Related Commands

None

3.1.20 switchport

Command Purpose

Use this command to configure a port to a bridge (layer 2) or routing (layer 3) mode.

Command Syntax

switchport

no switchport

Command Mode

Interface Configuration

Default

Switchport

Usage

When using this command to change the mode of a port, all bridge or routing configurations of this port will be cleared and not restored. By default, the port is a switchport.

Examples

This example shows how to configure a port to bridge mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport
```

This example shows how to configure a port to routing mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
```

Related Commands

None

3.1.21 switchport access allowed

Command Purpose

Use this command to configure whether the specified VLAN flow can pass this access port.

Command Syntax

switchport access allowed vlan (add | remove) VLAN_ID

Parameter	Parameter Description	Parameter Value
add	Allow the traffic from the vlan to pass the access port	-
remove	Not allow the traffic from the vlan to pass the access port	-

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan list connected with '-' and '' for example, "1-10,15,20,30-40"	1-4094

Command Mode

Interface Configuration

Default

1

Usage

This command is used to allow the traffic from the specific VLAN to pass the access port.

Examples

This example shows how to configure the specified VLAN flow pass through the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan add 10
```

This example shows how to allow the traffic from the vlan11 to pass the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan add 11
```

This example shows how to refuse the traffic from the vlan12 to pass the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan remove 12
```

Related Commands

switchport trunk allowed vlan (add vid | remove vid | all | none)

3.1.22 switchport access vlan

Command Purpose

Use this command to set the default VLAN for access port.

Command Syntax

switchport access vlan VLAN_ID

no switchport access vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	2-4094

Command Mode

Interface Configuration

Default

1

Usage

The port should be an access port by switchport mode access command before add to vlan by this command.

Examples

This example shows how to configure the access port to add to default vlan 10:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
```

This example shows how to configure the access port to restore to default vlan 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport access vlan
```

Related Commands

switchport trunk native

3.1.23 switchport mode access

Command Purpose

Use this command to configure the port work in access mode.

Command Syntax

switchport mode access

Command Mode

Interface Configuration

Default

Access Port

Usage

The access mode is usually used to connect the port to a terminal device, such as a PC.

When the mode is changed, both the MAC learnt dynamically and configured statically on the port will be cleared.

Examples

This example shows how to set the switchport mode to access:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
```

Related Commands

switchport mode trunk

3.1.24 switchport mode trunk

Command Purpose

Use this command to configure the port work in trunk mode.

Command Syntax

switchport mode trunk

Command Mode

Interface Configuration

Default

Access Port

Usage

The trunk mode is usually used to connect the port with other switch.

The trunk mode is can also used to connect the port with host device.

When the mode is changed, both the MAC learnt dynamically and configured statically on the port will be cleared.

Examples

This example shows how to return the port to default vlan 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
```

Related Commands

switchport mode access

3.1.25 switchport mode dot1q-tunnel

Command Purpose

Use this command to configure the port as QINQ port.

Command Syntax

switchport mode dot1q-tunnel

Command Mode

Interface Configuration

Default

Access Port

Usage

When port mode changed, all the dynamic FDB will be cleared.

Examples

This example shows how to configure the port to QINQ mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode dot1q-tunnel
```

Related Commands

switchport mode trunk

3.1.26 switchport trunk allowed

Command Purpose

Use this command to configure whether the specified VLAN flow can pass this trunk port.

Command Syntax

switchport trunk allowed vlan (add VLAN_ID | remove VLAN_ID | all | none)

Parameter	Parameter Description	Parameter Value
add VLAN_ID	allow the traffic from the specified vlan to transmit the trunk port. Vlan list connected with '-' and ',' for example, "1-10,15,20,30-40"	1-4094
remove VLAN_ID	do not allow the traffic from the specified vlan to transmit the trunk port. Vlan list connected with '-' and ',' for example, "1-10,15,20,30-40"	1-4094
all	allow the traffic from all the vlan to transmit the trunk port	-
none	do not allow the traffic from all the vlan to transmit the trunk port	-

Command Mode

Interface Configuration

Default

1

Usage

This command is used to allow traffic from specified VLAN to transmit the trunk port.

Examples

This example shows how to configure the specified VLAN flow pass through the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan add 10
```

This example shows how to refuse traffic from the specified VLAN to transmit the trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan remove 11,12
```

This example shows how to allow traffic from all vlan to transmit the trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan all
```

This example shows how to refuse traffic from all vlan to transmit the trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan none
```

Related Commands

switchport access allowed vlan (add | remove) vid

3.1.27 switchport trunk native vlan

Command Purpose

Use this command to set the default VLAN for trunk port.

Command Syntax

switchport trunk native vlan VLAN_ID

no switchport trunk native vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	2-4094

Command Mode

Interface Configuration

Default

1

Usage

The port should be a trunk port by switchport mode trunk command before add to vlan by this command.

Examples

This example shows how to configure default vlan 10 for trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
```

This example shows how to configure the trunk port to restore to default vlan 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport trunk native vlan
```

Related Commands

switchport access vlan vid

3.1.28 switchport port-bridge enable

Command Purpose

Use this command to enable port-bridge, allow homologous and homologous translate.

Command Syntax

switchport port-bridge enable
no switchport port-bridge enable

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to enable port-bridge:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport port-bridge enable
```

Related Commands

port-bridge enable

3.1.29 port-bridge enable

Command Purpose

Use this command to enable port-bridge support multicast and broadcast.

Command Syntax

port-bridge enable

no port-bridge enable

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to enable port-bridge support multicast and broadcast:

```
Switch# configure terminal
Switch(config)# port-bridge enable
```

Related Commands

switchport port-bridge enable

3.1.30 port-xconnect

Command Purpose

Use this command to set port cross connect destination interface. Use the no form of this command remove destination interface.

Command Syntax

port-xconnect destination-interface (IFPHYSICAL | IFAGG)

no port-xconnect destination-interface

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	Physical port	N/A
IFAGG	Aggregate port	-

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to set eth-0-1 port-xconnect destination interface to eth-0-2:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# interface eth-0-1
Switch(config-if)# port-xconnect destination-interface eth-0-2
```

Related Commands

3.1.31 carrier down-hold-time interval

Command Purpose

Use this command to set port down hold time. Use the no form of this command to remove port down hold time.

Command Syntax

carrier down-hold-time interval TIME

no carrier down-hold-time interval

Parameter	Parameter Description	Parameter Value
TIME	down hold time	0-500, unit is millisecond

Command Mode

Interface Configuration

Default

0

Usage

None

Examples

This example shows how to set 300ms for eth-0-1 down hold time:

```
Switch(config)# interface eth-0-1
Switch(config-if)# carrier down-hold-time interval 300
```

Related Commands

None

3.1.32 Mtu

Command Purpose

Use this command to configure the maximum transmit unit for this interface.

Command Syntax

mtu VALUE

Parameter	Parameter Description	Parameter Value
VALUE	MTU	68-9216

Command Mode

Interface Configuration

Default

1500

Usage

This command is only allowed to be used in layer3 interface.

Examples

This example shows how to configure MTU 1600 for VLAN interface 10:

```
Switch# configure terminal
Switch(config)# interface vlan10
Switch(config-if)#mtu 1600
```

Related Commands

None

3.1.33 wavelength freq

Command Purpose

Use this command to configure the wavelength of tunable fiber used on this interface. Use the no form of this command restore to the default value. Each wavelength corresponds to a fixed frequency and the command sets the wavelength by configuring the frequency.

Command Syntax

wavelength freq FREQ

no wavelength freq

Parameter	Parameter Description	Parameter Value
FREQ	fiber frequency	19110-19615, step is 5

Command Mode

Interface Configuration

Default

19340

Usage

The configurations of this command only effective when the tunable fiber is inserted on this interface.

Examples

This example shows how to configure wavelength freq 19120 for interface 10:

```
Switch# configure terminal
Switch(config)# interface eth-0-10
Switch(config-if)#wavelength freq 19120
```

Related Commands

None

3.2 Interface Errdisable Commands

3.2.1 errdisable detect

Command Purpose

Use the interface errdisable detects configuration command to enable errdisable detection. Use the no form of this command to disable errdisable detection.

Command Syntax

errdisable detect reason (link-flap | fdb-loop | uddld)

no errdisable detect reason (link-flap | fdb-loop | udld)

Parameter	Parameter Description	Parameter Value
link-flap	Enable detect Link flap error	-
fdb-flap	Enable detect FDB error	-
udld	Enable detect UDLD error	-

Command Mode

Global Configuration

Default

link-flap Enable

fdb-loop Enable

udld Enable

Usage

None

Examples

This example shows how to enable errdisable detect link flap:

```
Switch# configure terminal
Switch(config)# errdisable detect reason link-flap
```

This example shows how to disable errdisable detect link flap:

```
Switch# configure terminal
Switch(config)# no errdisable detect reason link-flap
```

Related Commands

show errdisable detect

3.2.2 errdisable recovery interval

Command Purpose

Use this command to set the specified timer to recover from the errdisable state. Use the no form of this command to restore to the default interval.

Command Syntax

errdisable recovery interval RANGE

no errdisable recovery interval

Parameter	Parameter Description	Parameter Value
RANGE	Recovery interval range	30-86400, unit:second

Command Mode

Global Configuration

Default

300 seconds

Usage

Default recovery interval is 300 seconds.The change of interval will not affect already started errdisable recovery timer.If not enable errdisable recovery, the port will not recovery automatic.

Examples

This example shows how to set errdisable recovery to 30 seconds:

```
Switch# configure terminal
Switch(config)# errdisable recovery interval 30
```

This example shows how to set errdisable recovery to default values:

```
Switch# configure terminal
Switch(config)# no errdisable recovery interval
```

Related Commands

errdisable recovery reason

show errdisable recovery

3.2.3 errdisable fdb-loop count

Command Purpose

Use this command to set FDB-loop check parameter. Use the no form of this command to restore to the default count.

Command Syntax

errdisable fdb-loop count COUNT

no errdisable fdb-loop count

Parameter	Parameter Description	Parameter Value
COUNT	Set the FDB-loop times, default 10.	3-50

Command Mode

Global Configuration

Default

10

Usage

Period is 60s.

Examples

This example shows how to set count 5:

```
Switch# configure terminal
Switch(config)# errdisable fdb-loop count 5
```

Related Commands

errdisable recovery reason

show errdisable recovery

show errdisable fdb-loop

3.2.4 errdisable fdb-loop exclude-vlan

Command Purpose

Use this command to set FDB-loop vlan white list. Use the no form of this command to detect the specified vlan.

Command Syntax

errdisable fdb-loop exclude-vlan VLAN_LIST

no errdisable fdb-loop exclude-vlan

Parameter	Parameter Description	Parameter Value
VLAN_LIST	Set the vlan list that not need FDB-loop detect	Connected with '-' and ',' for example, "1-10,15,20,30-40"

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set exclude-vlan 1,5-7:

```
Switch# configure terminal
Switch(config)# errdisable fdb-loop exclude-vlan 1,5-7
```

Related Commands

show errdisable fdb-loop

3.2.5 errdisable recovery reason

Command Purpose

Use this command to enable error disable detection for a specified cause or all cause. Use the no form of this command to disable the error disable feature.

Command Syntax

errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection)

no errdisable recovery reason (all | bpduguard | bpduloop | port-security | link-flap | link-monitor-failure | oam-remote-failure | udld | fdb-loop | loopback-detection)

Parameter	Parameter Description	Parameter Value
all	Enable timer to recover from all reason	-
bpduguard	Enable timer to recover from BPDU Guard error disable state	-
bpduloop	Enable timer to recover from BPDU Loopback error disable state	-
port-security	Enable timer to recover from Port security failure	-
link-flap	Enable timer to recover from Link flap failure	-
link-monitor-failure	Enable timer to recover from link monitoring failure	-
oam-remote-failure	Enable timer to recover from OAM detected remote failure	-
udld	Enable timer to recover from UDLD failure	-
fdb-loop	Enable timer to recover from FDB loop failure	-
loopback-detection	Enable timer to recover from loopback detection error disable state	-

Command Mode

Global Configuration

Default

Disabled

Usage

The change of reason will not affect those interfaces have already enter errdisable state.

Examples

This example shows how to enable link flap errdisable recovery:

```
Switch# configure terminal
Switch(config)# errdisable recovery reason link-flap
```

This example shows how to disable link flap errdisable recovery:

```
Switch# configure terminal
Switch(config)# no errdisable recovery reason link-flap
```

Related Commands

errdisable recovery interval

show errdisable recovery

3.2.6 errdisable flap**Command Purpose**

Use this command to set the parameters for link-flap error disable. Use the no form of this command to restore to default value.

Command Syntax

errdisable flap reason link-flap COUNT SECONDS

no errdisable flap reason link-flap COUNT SECONDS

Parameter	Parameter Description	Parameter Value
link-flap	Configure link flap conditions	-
COUNT	Max flap count	1-100, unit:times
SECONDS	Flap count time in seconds	1-120, unit:second

Command Mode

Global Configuration

Default

count : 10, seconds :10

Usage

Only the link flap can be detected. <1-100> is the threshold of flap count, and <1-120> is the count time in seconds for flap count. If the errdisable detect link flap is enabled, will result in link flap errdisable, otherwise, will only print a message in log.

Examples

This example shows how to set link flap conditions to 20 times in 60 seconds:

```
Switch# configure terminal
Switch(config)# errdisable flap reason link-flap 20 60
```

This example shows how to disable link flap conditions to default:

```
Switch# configure terminal
Switch(config)# no errdisable flap reason link-flap
```

Related Commands

show errdisable flap

3.2.7 show errdisable detect

Command Purpose

Use this command to display the error disable detection reason.

Command Syntax

showCommand Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the error disable detection reason:w errdisable detect

```
DUT1# show errdisable detect
```

ErrDisable Reason	Detection status
-----	-----
bpduguard	Enabled
bpduloop	Enabled
link-monitor-failure	Enabled
oam-remote-failure	Enabled
port-security	Enabled
link-flap	Enabled
monitor-link	Enabled
udld	Disabled
fdb-loop	Disabled
loopback-detection	Enabled
reload-delay	Enabled

Related Commands

errdisable detect

3.2.8 show errdisable recovery

Command Purpose

Use this command to display the error disable recovery timer.

Command Syntax

show errdisable recovery

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the error disable recovery:

```
Switch# show errdisable recovery
```

ErrDisable Reason	Timer Status
bpdu-guard	Disabled
bpdu-loop	Disabled
link-monitor-failure	Disabled
oam-remote-failure	Disabled
port-security	Disabled
link-flap	Disabled
udld	Disabled
fdb-loop	Disabled
loopback-detection	Disabled

Timer interval: 300 seconds

Related Commands

errdisable recovery interval

errdisable recovery reason

3.2.9 show errdisable flap

Command Purpose

Use this command to display error disable link flap parameters.

Command Syntax

```
show errdisable flap
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the flap configuration:

```
Switch# show errdisable flap
```

ErrDisable Reason	Flaps	Time (sec)
link-flap	10	10

Related Commands

errdisable flap

3.2.10 show errdisable fdb-loop

Command Purpose

Use this command to display error disable fdb-loop parameters.

Command Syntax

show errdisable fdb-loop

Command Mode

Privileged EXEC

Default

None

Usage

When mac address migrates from one port to another port for 10 times in one minute, this mac address is considered as flapping and switch would print a flapping log for users. The log would be printed every 10 minutes.

Examples

This example shows how to display the fdb-loop configuration:

```
Switch# show errdisable fdb-loop
```

```
Errdisable FDB loop information
```

Exclude VLAN-list	: N/A
Detecting count	: 10
Detecting period	: 60s
Printing log period	: 600s

Related Commands**3.2.11 errdisable fdb-loop trust****Command Purpose**

Use this command to set trust mode on interface, and this interface would not be set error disable by fdb-loop detection.

Use the no form of this command to disable the error disable feature.

Command Syntax

errdisable fdb-loop trust

no errdisable fdb-loop trust

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to set trust mode on interface for fdb flap:

```
DUT1(config)# interface eth-0-1
DUT1(config-if)# errdisable fdb-loop trust
```

This example shows how to unset trust mode on interface for fdb flap:

```
DUT1(config)# interface eth-0-1
DUT1(config-if)# no errdisable fdb-loop trust
```

Related Commands

None

3.3 MAC Address Table Commands

3.3.1 mac-address-table ageing-time

Command Purpose

Use the mac-address-table aging-time global configuration command on the switch to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the no form of this command to return to the default setting. The aging time applies to all VLANs.

Command Syntax

MAC_ADDRESS-table ageing-time SECONDS

no MAC_ADDRESS-table ageing-time

Parameter	Parameter Description	Parameter Value
SECONDS	Aging time	0, 10-1000000, 0 means that MAC aging function does not work, unit:second

Command Mode

Global Configuration

Default

The default is 300 seconds

Usage

If packets are not received continuously, user can increase the aging time to make the system recording the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

Examples

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch# configure terminal
Switch(config)# mac-address-table ageing-time 200
```

Related Commands

show mac address-table ageing-time

3.3.2 mac-address-table hardware-learning

Command Purpose

Use the mac-address-table hardware-learning enable global configuration command on the switch to study FDB without software. Use the no form of this command to return to the default setting.

Command Syntax

MAC_ADDRESS-table hardware-learning enable

no MAC_ADDRESS-table hardware-learning enable

Command Mode

Global Configuration

Default

Disable

Usage

Hardware learning is more faster than software learning.

Examples

This example shows how to enable hardware learning:

```
Switch# configure terminal
Switch(config)# mac-address-table hardware-learning enable
```

Related Commands

None

3.3.3 mac-address-table forward

Command Purpose

Use the mac-address-table forward global configuration command on the switch to add static addresses to the MAC address table. Use the no form of this command to remove static entries from the table.

Command Syntax

MAC_ADDRess-table MAC_ADDR forward (IFNAME | eps EPS_ID | remote-vtep REMOTE_VTEP_ID | smart-link SMART_LINK_ID) vlan VLAN_ID

no MAC_ADDRess-table MAC_ADDR forward (IFNAME | eps EPS_ID | remote-vtep REMOTE_VTEP_ID | smart-link SMART_LINK_ID) vlan VLAN_ID

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface	Mac address in HHHH.HHHH.HHHH format
IFNAME	Interface to which the received packet is forwarded.	Valid interfaces include physical ports and link aggregation ports
VLAN_ID	Specify the VLAN for which the packet with the specified MAC address is received.	1-4094
EPS_ID	EPS protection group.	1-2048
REMOTE_VTEP_ID	Remote VTEP	1-65535
SMART_LINK_ID	Smart-Link Group	1-16

Command Mode

Global Configuration

Default

None

Usage

The static address entries which are added by this command are not aged.

Examples

This example shows how to add the static address c2f3220a12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch# configure terminal
Switch(config)# mac-address-table c2f3.220a.12f4 forward eth-0/1 vlan 4
```

Related Commands

show mac address-table

3.3.4 mac-address-table discard

Command Purpose

Use the mac-address-table discard global configuration command on the switch to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the no form of this command to return to the default setting.

Command Syntax

MAC_ADDRes-table MAC_ADDR discard

no MAC_ADDRes-table MAC_ADDR discard

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Source or Destination MAC address (unicast) to add to the address filtering table	-

Command Mode

Global Configuration

Default

None

Usage

Follow these guidelines when using this feature:

Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.

Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3220a12f4. When a packet is received with this MAC address as its source or destination, the packet is dropped:

```
Switch# configure terminal
Switch(config)# mac-address-table c2f3.220a.12f4 discard
```

Related Commands

mac-address-table forward

3.3.5 clear mac address-table

Command Purpose

Use the clear mac address-table privileged EXEC command on the switch to delete all dynamic(or static, or multicast) addresses, or all dynamic(or static, or multicast) addresses on a particular interface, or all dynamic(or static, or multicast) addresses on a particular VLAN from the MAC address table.

Command Syntax

clear mac address-table (static | dynamic | multicast) (address MAC_ADDR | interface IFNAME | vlan VLAN_ID)

Parameter	Parameter Description	Parameter Value
dynamic	Delete the dynamic MAC address	-
static	Delete the static MAC address	-
multicast	Delete the multicast MAC address	-
address MAC_ADDR	Delete the specified MAC address	Mac address in HHHH.HHHH.HHHH format

Parameter	Parameter Description	Parameter Value
interface IFNAME	Delete all MAC addresses on the specified physical port or link aggregation port	Support physical/aggregation ports
vlan VLAN_ID	Delete all MAC addresses for the specified VLAN.	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands

show mac address-table

3.3.6 port-bridge**Command Purpose**

Use this command to support to forward packets with the src-mac and dset-mac learned by the same port.

Command Syntax

switchport port-bridge enable

no switchport port-bridge enable

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to enable port-bridge function:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport port-bridge enable
```

Related Commands**3.3.7 show mac address-table ageing-time****Command Purpose**

Use the show mac address-table ageing-time privileged EXEC command to display the aging time of all address table instances on all VLANs.

Command Syntax

show mac address-table ageing-time

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table ageing-time command:

```
Switch# show mac address-table ageing-time
MAC address table ageing time is 300 seconds
```

Related Commands

mac-address-table ageing-time

3.3.8 show mac address-table**Command Purpose**

Use the show mac address-table privileged EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

Command Syntax

show mac address-table (dynamic | static | multicast |) (address MAC_ADDR | interface IFNAME | vlan VLAN_ID |)

Parameter	Parameter Description	Parameter Value
dynamic	Display the dynamic MAC address	-
static	Display the static MAC address	-
multicast	Display the multicast MAC address	-
address MAC_ADDR	Display the specified MAC address	Mac address in HHHH.HHHH.HHHH format
interface IFNAME	Display all MAC addresses on the specified physical port or link aggregation port	Support physical/aggregation ports
vlan VLAN_ID	Display all MAC addresses for the specified VLAN.	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table command:

```
Switch# show mac address-table
```

Mac Address Table

```

(*) - Security Entry      (M) - MLAG Entry
(MO) - MLAG Output Entry  (MI) - MLAG Input Entry
Vlan    Mac Address      Type      Ports
-----
1       0000.0000.0001    static    eth-0-2
1       0000.0001.0003    static(*) eth-0-1
1       0000.0001.0002    static(*) eth-0-1
2       26fc.72e5.0100    dynamic(*) eth-0-9
1       0100.0000.0001    static    eth-0-2

```

Related Commands

mac-address-table

3.3.9 show mac address-table hardware

Command Purpose

Use the show mac address-table hardware privileged EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN in hardware.

Command Syntax

```
show mac address-table hardware ( dynamic | static | ) ( address MAC_ADDR | interface IFNAME | vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
dynamic	Display the dynamic MAC address	-
static	Display the static MAC address	-
address MAC_ADDR	Display the specified MAC address	Mac address in HHHH.HHHH.HHHH format
interface IFNAME	Display all MAC addresses on the specified physical port or link aggregation port	Support physical/aggregation ports
vlan VLAN_ID	Display all MAC addresses for the specified VLAN.	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table hardware command:

```
Switch# show mac address-table hardware
```

Mac Address Table

```

(*) - Security Entry      (M) - MLAG Entry
(MO) - MLAG Output Entry  (MI) - MLAG Input Entry

```

Vlan	Mac Address	Type	Ports
1	0000.0000.0001	static	eth-0-2
1	0000.0001.0003	static(*)	eth-0-1
1	0000.0001.0002	static(*)	eth-0-1
2	26fc.72e5.0100	dynamic(*)	eth-0-9
1	0100.0000.0001	static	eth-0-2

Related Commands

mac-address-table

3.3.10 show mac address-table count

Command Purpose

Use the show mac address-table count privileged EXEC command to display the number of addresses present in all VLANs.

Command Syntax

show mac address-table count

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table count command:

```
Switch# show mac address-table count

Dynamic Address Count   :    1   (Security: 0)
Static  Address Count   :    1   (Security: 0)
Total Mac Addresses     :    2   (Security: 0)
```

Related Commands

show mac address-table

3.3.11 show mac address-table hardware count

Command Purpose

Use the show mac address-table count privileged EXEC command to display the number of addresses present in all VLANs in hardware.

Command Syntax

show mac address-table hardware count

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table hardware count command:

```
Switch# show mac address-table hardware count
```

```
MAC address count in hardware table:  
(Include MAC security entry)
```

```
-----  
Dynamic Address Count   :    0  
Static Address Count    :    0  
Total Mac Addresses     :    0
```

Related Commands

show mac address-table hardware

3.3.12 show mac address-table add-fdb-fail

Command Purpose

Use the show mac address-table add-fdb-fail privileged EXEC command to display all failed static FDB entries when adding FDB table in chip for hash conflict.

Command Syntax

show mac address-table add-fdb-fail

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac address-table add-fdb-fail command:

```
Switch# show mac address-table add-fdb-fail
```

Vlan	Mac Address	Type	Ports
1	0000.0000.0001	static	eth-0-1
1	0000.0000.0002	static	eth-0-2

Related Commands

show mac address-table

3.3.13 show mac-filter address-table

Command Purpose

Use the show mac-filter address-table privileged EXEC command to display the number of filter addresses present in all VLANs.

Command Syntax

show mac-filter address-table

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is an example of output from the show mac-filter address-table command:

```
Switch# show mac-filter address-table
```

MAC Filter Address Table

```
-----
Current count      : 0
Max count          : 128
Left count         : 128
Filter address list :
-----
```

Related Commands

show mac address-table

3.3.14 show resource mac-filter**Command Purpose**

Use this command to display the resource statistic used by mac-filter.

Command Syntax

show resource mac-filter

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource mac-filter command:

```
Switch# show resource mac-filter
```

MAC-FILTER

Resource	Used	Capability
=====		
Blackhole MAC Addresses	0	128

Related Commands

show resource static-fdb

3.3.15 show resource static-fdb**Command Purpose**

Use this command to display the resource statistic used by static FDB.

Command Syntax

show resource static-fdb

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource static-fdb command:

```
Switch# show resource static-fdb
```

```
STATIC-FDB
```

Resource	Used	Capability
=====		
Static FDB	0	1024

Related Commands

show resource mac-filter

3.4 VLAN Commands

3.4.1 vlan database

Command Purpose

Use this command to enter VLAN configure mode.

Command Syntax

vlan database

Command Mode

Global Configuration

Default

None

Usage

When you try to create or remove VLAN, you must use this command to enter VLAN configure mode first. To exit VLAN configure mode, use exit command.

Examples

This example shows how to enter VLAN configure mode:

```
Switch# configureterminal
Switch(config)# vlan database
Switch(config-vlan)#
```

This example shows how to exit VLAN configure mode:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# exit
Switch(config)#
```

Related Commands

exit

3.4.2 Vlan

Command Purpose

Use the vlan VLAN configuration command to configure VLAN characteristics for a VLAN in the VLAN database. Use the no form of this command to delete a VLAN.

Command Syntax

vlan VLAN_ID (name NAME |) (state (enable | disable) |)

no vlan VLAN_ID

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	1-4094
NAME	the name for specific vlan,	A string with no more than 31 characters
enable	set the operational state of the VLAN to enable, and it is enabled by default	-
disable	set the operational state of the VLAN to disable	-

Command Mode

VLAN Configuration

Default

VLAN 1 is the default VLAN and all ports have been added to it by default.

Usage

Default VLAN 1 can not be removed.

Examples

This example shows how to create VLAN 11 and named it to "vlan11":

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 11 name vlan11 state enable
```

This example shows how to remove VLAN 11:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# no vlan 11
```

Related Commands

vlan VLAN_LIST

show vlan vlan

show vlan all

3.4.3 vlan port

Command Purpose

Use the vlan VLAN configuration command to add VLAN to port. Use the no form of this command to remove VLAN from port.

Command Syntax

vlan VLAN_ID port slot SLOT_ID port PORT_ID

no vlan VLAN_ID port slot SLOT_ID port PORT_ID

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	1-4094
SLOT_ID	The slot id of the port	-
PORT_ID	The port id of the port	-

Command Mode

VLAN Configuration

Default

None

Usage

None

Examples

This example shows how to add VLAN 11 to eth-0-4:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 11 port slot 0 port 4
```

Related Commands

vlan VLAN_LIST

3.4.4 vlan VLAN_LIST**Command Purpose**

Use the vlan VLAN_LIST configuration command to add a normal-range VLANs to the VLAN database.

Command Syntax

vlan VLAN_LIST

no vlan VLAN_LIST

Parameter	Parameter Description	Parameter Value
VLAN_LIST	vlan list	vlan list connected with '-' and ',' for example, "1-10,15,20,30-40"

Command Mode

VLAN Configuration

Default

Vlan 1 is the default vlan and all ports have been added to it by default.

Usage

The vlan list should be connected with '-' and ',' the value should be in the range of <1-4094> and should be ascending order.

Default VLAN 1 can not be removed.

Examples

This example shows how to add vlans of "100,200,300-400":

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 100,200,300-400
```

This example shows how to remove vlans of "100,200,300-400":


```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# no vlan 100,200,300-400
```

Related Commands

vlan <1-4094>

show vlan vlan

show vlan all

3.4.5 show vlan

Command Purpose

Use this command to display specific vlan information.

Command Syntax

show vlan VLAN_ID

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display VLAN property including name, state, stp id, DSCP, member ports.

Examples

This example shows how to display the information on VLAN 11:

```
Switch# show vlan 11
```

VLAN ID	Name	State	STP ID	Member ports
(u)-Untagged, (t)-Tagged				
11	VLAN0011	ACTIVE	0	eth-0-3(u) eth-0-4(t)

Related Commands

show vlan all

3.4.6 show vlan all

Command Purpose

Use this command to show the information of all the VLAN.

Command Syntax

show vlan all

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display all VLAN property including name, state, stp id, DSCP, member ports.

Examples

This example shows how to display the information on VLAN all:

```
Switch# show vlan all
```

VLAN ID	Name	State	STP ID	Member ports
(u)-Untagged, (t)-Tagged				
1	default	ACTIVE	0	eth-0-1(u) eth-0-2(u) eth-0-4(t) eth-0-5(u)
11	VLAN0011	ACTIVE	0	eth-0-3(u) eth-0-4(t)

Related Commands

```
show vlan vlan
```

3.4.7 show vlan brief**Command Purpose**

Use this command to show the brief information on VLAN.

Command Syntax

```
show vlan brief
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display all VLAN information for all bridges, including static and dynamic.

Examples

This example shows how to display the brief information on VLAN:

```
Switch# show vlan brief
```

VLAN ID	Name	State	STP ID	Member ports
(u)-Untagged, (t)-Tagged				
1	default	ACTIVE	0	eth-0-1(u) eth-0-2(u) eth-0-4(u) eth-0-5(u)
10	VLAN0010	ACTIVE	0	eth-0-3(u)

Related Commands

```
show vlan vlan
```

3.4.8 show interface switchport

Command Purpose

Use this command to show the vlan configurations on all bridge ports or a bridge port.

Command Syntax

show interface switchport { interface IFNAME | }

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support aggregation and physical ports

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display one or all VLAN's L2 configurations.

Examples

This example shows how to display the vlan configurations on all bridge ports or a bridge port:

```
Switch# show interface switchport interface eth-0-1
```

```
Interface name      : eth-0-1
Switchport mode     : access
Ingress filter      : enable
Acceptable frame types : vlan-untagged only
Default Vlan        : 1
Configured Vlans     : 1

Interface name      : eth-0-2
Switchport mode     : access
Ingress filter      : enable
Acceptable frame types : vlan-untagged only
Default Vlan        : 1
Configured Vlans     : 1
```

Related Commands

switchport mode access

switchport mode trunk

3.4.9 switchport access allowed

Command Purpose

Use this command to allow or remove the access port to the specifid vlan

Command Syntax

switchport access allowed vlan (add | remove) VLAN_ID_LIST

Parameter	Parameter Description	Parameter Value
add	add the port to the specified vlan	-
remove	remove the port from the specified vlan	-

Parameter	Parameter Description	Parameter Value
VLAN_ID_LIST	vlan list	Connected with '-' and ',' for example, "1-10,15,20,30-40"

Command Mode

Interface Configuration

Default

None

Usage

This command used to allow or forbid the port transmit in specified vlan.

Examples

This example shows how to add the access port to vlan11:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan add 11
```

This example shows how to remove the access port to vlan12:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access allowed vlan remove 12
```

Related Commands

switchport trunk allowed

3.4.10 switchport access vlan

Command Purpose

Use this command to add port to a specified. Use the no form of this command to add port to vlan1.

Command Syntax

switchport access vlan VLAN_ID

no switchport access vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	2-4094

Command Mode

Interface Configuration

Default

All ports are default in vlan 1

Usage

Used the switchport mode access command to switch the port to access mode before use this command.

Examples

This example shows how to add the access port to vlan11:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport access vlan 11
```

This example shows how to revert the port to vlan1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport access vlan
```

Related Commands

switchport mode access

3.4.11 switchport mode access**Command Purpose**

Use this command to switch port to access mode.

Command Syntax

switchport mode access

Command Mode

Interface Configuration

Default

None

Usage

Access mode used to connect terminal, e.g:PC.The FDB on the port will be cleared when switch the port mode.

Examples

This example shows how to set the port to access mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
```

Related Commands

switchport mode trunk

3.4.12 switchport mode trunk**Command Purpose**

Use this command to switch port to trunk mode.

Command Syntax

switchport mode trunk

Command Mode

Interface Configuration

Default

None

Usage

Trunk mode used to connect switch device or terminal.The FDB on the port will be cleared when switch the port mode.

Examples

This example shows how to set the port to trunk mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
```

Related Commands

switchport mode access

3.4.13 switchport trunk allowed

Command Purpose

Use this command to allow or remove the trunk port to the specified

Command Syntax

switchport trunk allowed vlan (add VLAN_ID_LIST | remove VLAN_ID_LIST | all | none)

no switchport trunk

Parameter	Parameter Description	Parameter Value
VLAN_ID_LIST	vlan list	Connected with '-' and ',' for example, "1-10,15,20,30-40"
add	add the port to the specified vlan	-
remove	remove the port from the specified vlan	-
all	add the port to all vlans	-
none	remove the port from all vlans	-

Command Mode

Interface Configuration

Default

None

Usage

This command is used to allow or forbid the port to transmit in specified vlans.

Examples

This example shows how to add the port to vlans 11,12:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan add 11,12
```

This example shows how to remove the port from vlans 11,12:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan remove 11,12
```

This example shows how to allow the port to transmit in all vlans:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan all
```

This example shows how to forbid the port to transmit in all vlans:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk allowed vlan none
```

Related Commands

switchport access allowed

3.4.14 switchport trunk native**Command Purpose**

Use this command to configure the default VLAN for this trunk port.

Command Syntax

switchport trunk native vlan VLAN_ID

no switchport trunk native vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	An existing Vlan id	2-4094

Command Mode

Interface Configuration

Default

vlan 1

Usage

This command is used to set the native VLAN for sending and receiving untagged traffic.

Examples

This example shows how to set the native vlan to vlan 10 on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk native vlan 10
```

This example shows how to return the native vlan to default on the interface:

```
Switch# configureterminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport trunk native vlan
```

Related Commands

switchport trunk allowed

3.4.15 switchport trunk unatgged vlan**Command Purpose**

Use this command to strip the packets vlan tag out of this port.

Command Syntax

switchport trunk untagged vlan VLAN_ID_LIST

no switchport trunk untagged vlan VLAN_ID_LIST

Parameter	Parameter Description	Parameter Value
VLAN_ID_LIST	vlan list	Connected with '-' and ',' for example, "1-10,15,20,30-40"

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to allocate the needing strip vlan tag on the interface.:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk untagged vlan 1-2
```

Related Commands

None

3.4.16 vlan bridge disable**Command Purpose**

Use this command to disable bridge function on specific VLAN. To enable it, use the no form of this command.

Command Syntax

vlan VLAN_ID bridge disable

no vlan vlan bridge disable

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	1-4094

Command Mode

VLAN Configuration

Default

Vlan bridge enable

Usage

None

Examples

This example shows how to disable bridge function on VLAN 2:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10 bridge disable
```

This example shows how to enable bridge function on VLAN 2:

```
Switch# configureterminal
Switch(config)# vlan database
Switch(config-vlan)# no vlan 10 bridge disable
```

Related Commands

None

3.4.17 vlan statistics enable

Command Purpose

Use this command to enable the statistics of VLAN.

To disable the statistics, use the no form of this command.

Command Syntax

vlan VLAN_ID statistics enable

no vlan VLAN_ID statistics enable

Parameter	Parameter Description	Parameter Value
VLAN_ID	An existing Vlan id	1-4094

Command Mode

VLAN Configuration

Default

inactive

Usage

none

Examples

This example shows how to enable the statistics of vlan 2:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2 statistics enable
```

This example shows how to disable the statistics of vlan 2:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)#no vlan 2 statistics enable
```

Related Commands

vlan statistics interval

clear vlan statistics

show vlan vlan statistics

3.4.18 vlan statistics interval

Command Purpose

Use this command to set sample interval.

To restore to default value, use the no form of this command.

Command Syntax

vlan statistics interval VALUE

no vlan statistics intval

Parameter	Parameter Description	Parameter Value
VALUE	Sample interval	5-600, unit:second

Command Mode

VLAN Configuration

Default

10s

Usage

none

Examples

This example shows how to set sample interval:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan statistics interval 20
```

Related Commands

vlan statistics enable

clear vlan statistics

show vlan vlan statistics

3.4.19 clear vlan statistics**Command Purpose**

Use this command to clear statistics information.

Command Syntax

clear vlan VLAN_ID statistics

Parameter	Parameter Description	Parameter Value
VLAN_ID	An existing Vlan id	1-4094

Command Mode

Privileged EXEC

Default

none

Usage

none

Examples

This example shows how to clear vlan statistics:

```
Switch# clear vlan 2 statistics
```

Related Commands

vlan statistics enable

vlan statistics interval

show vlan vlan statistics

3.4.20 show vlan statistics**Command Purpose**

Use this command to show statistics information.

Command Syntax

show vlan VLAN_ID statistics

Parameter	Parameter Description	Parameter Value
VLAN_ID	An existing Vlan id	1-4094

Command Mode

Privileged EXEC

Default

none

Usage

none

Examples

This example shows how to show vlan statistics:

```
Switch# show vlan 2 statistics
```

```
VLAN: 2
```

Item	Packets
Inbound:	3654365
Outbound:	3654365

Related Commands

vlan statistics enable

vlan statistics interval

3.4.21 show resource vlan-stats

Command Purpose

Use this command to show the resource statistic used by vlan statistics.

Command Syntax

show resource vlan-stats

Command Mode

Privileged EXEC

Default

none

Usage

none

Examples

This example shows how to show resource used by vlan statistics:

```
Switch# show resource vlan-stats
```

```
VLAN-STATS
```

Resource	Used	Capability
Applied VLAN Stats Entry	1	128

Related Commands

vlan statistics enable

3.5 Voice VLAN Commands

3.5.1 voice vlan

Command Purpose

Use this command to specific VLAN as VOICE VLAN.

Command Syntax

voice vlan VLAN_ID

no voice vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan id	2-4094

Command Mode

Global Configuration

Default

Voice VLAN is disable

Usage

This command is enabled VOICE VLAN.

Examples

This example shows how to enable VLAN 2 as VOICE VLAN:

```
Switch# configure terminal
Switch(config)# voice vlan 2
```

Related Commands

None

3.5.2 voice vlan security enable

Command Purpose

Use this command to enable VOICE VLAN security.

Command Syntax

voice vlan security enable

no voice vlan security enable

Command Mode

Global Configuration

Default

By default the mode is security.

Usage

If the security is enabled, all the packet that whose MAC is mismatched with OUI will be dropped in VOICE VLAN.

Examples

This example shows how to enable security:

```
Switch# configure terminal
Switch(config)# voice vlan security enable
```

Related Commands

show voice vlan state

3.5.3 voice vlan set cos to

Command Purpose

Use this command to set COS for VOICE packet.

Command Syntax

voice vlan set cos to COS

no voice vlan set cos

Parameter	Parameter Description	Parameter Value
COS	cos value	0-7

Command Mode

Global Configuration

Default

By default the phb is 5

Usage

This command is used to set COS for VOICE packet in global configuration.

Examples

This example shows how to set cos to 7:

```
Switch# configureterminal
Switch(config)# voice vlan set cos to 7
```

Related Commands

show voice vlan state

3.5.4 voice vlan mac-address

Command Purpose

Use this command to add OUI to system.

Command Syntax

voice vlan mac-address MAC MASK description LINE

no voice vlan mac-address MAC

Parameter	Parameter Description	Parameter Value
MAC	Source MAC address (unicast or multicast) to add to the address table	MAC Address in HHHH.HHHH.HHHH format
MASK	The MASK for the Source MAC	MAC Mask in HHHH.HHHH.HHHH format

Parameter	Parameter Description	Parameter Value
LINE	The description for this OUI	Up to 63 characters

Command Mode

Global Configuration

Default

There are 5 default OUI in the system.:

0003-6b00-0000 Cisco phone

000f-e200-0000 H3C Aolynk phone

00d0-1e00-0000 Pingtel phone

00e0-7500-0000 Polycom phone

00e0-bb00-0000 3Com phone

Usage

This command is used to add OUI to system database. The packet will be considered as VOICE VLAN packet when the source MAC match the OUI.

Examples

This example shows how to add OUI to system:

```
Switch# configure terminal
Switch(config)# voice vlan mac-address 0034.3400.0000 FFFF.FF00.0000 description test
```

Related Commands

show voice vlan state

3.5.5 voice vlan enable

Command Purpose

Use this command to enable VOICE VLAN on port.

Command Syntax

voice vlan enable

no voice vlan enable

Command Mode

Interface Configuration

Default

VOICE VLAN is disable on port

Usage

This command is used to enable VOICE VLAN on port.

Examples

This example shows how to enable VOICE VLAN on port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# voice vlan enable
```

Related Commands

show voice vlan state

3.5.6 show voice vlan state

Command Purpose

Use this command to show the current status of VOICEC VLAN.

Command Syntax

show voice vlan state

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show the current status of VOICEC VLAN.

Examples

This example shows how to show the current status of VOICEC VLAN:

```
Switch# show voice vlan state
```

Related Commands

voice vlan enable

3.6 Link Aggregation Commands

3.6.1 channel-group

Command Purpose

Use this command to assign a port to a channel group. Use the no form of this command to remove a port from a channel group.

Command Syntax

channel-group GROUP_NUMBER mode (active | passive)

no channel-group

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	1-63
active	Enable initiation of LACP negotiation on a port	-
passive	Disable initiation of LACP negotiation on a port	-

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to assign a port to a channel group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# channel-group 1 mode active
```

This example shows how to remove a port from an channel group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no channel-group
```

Related Commands

None

3.6.2 static-channel-group

Command Purpose

Use this command to assign a port to a static channel group. Use the no form of this command to remove a port from a static channel group.

Command Syntax

static-channel-group GROUP_NUMBER

no static-channel-group

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to assign a port to a static channel group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# static-channel-group 1
```

This example shows how to remove a port from a static channel group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no static-channel-group
```

Related Commands

None

3.6.3 distribute-weight

Command Purpose

Use this command to configure the distribute-weight of member for the static channel group or the Link Aggregation Control Protocol (LACP). Use the no form of this command to return to the default setting.

Command Syntax

distribute-weight WEIGHT

Parameter	Parameter Description	Parameter Value
WEIGHT	Distribute-weight	1-256

Command Mode

Interface Configuration

Default

1

Usage

Distribute-weight is only supported in non-selfing-healing of static load-balance-mode member port, and the total weights of member ports cannot exceed the maximum number of member ports.

Examples

This example shows how to configure the distribute-weight 10 for member:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# static-channel-group 1
Switch(config-if)# distribute-weight 10
```

This example shows how to return to the default setting:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# static-channel-group 1
Switch(config-if)# no distribute-weight
```

Related Commands

None

3.6.4 lacp port-priority

Command Purpose

Use this command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the no form of this command to return to the default setting.

Command Syntax

lacp port-priority PRIORITY

Parameter	Parameter Description	Parameter Value
PRIORITY	LACP port priority	1-65535

Command Mode

Interface Configuration

Default

32768

Usage

None

Examples

This example shows how to configure the port priority 100 for the Link Aggregation Control Protocol (LACP) member:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lacp port-priority 100
```

This example shows how to return to the default setting:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no lacp port-priority
```

Related Commands

None

3.6.5 lacp timeout**Command Purpose**

Use this command to configure the port timeout for the Link Aggregation Control Protocol (LACP). Use the no form of this command to return to the default setting.

Command Syntax

lacp timeout (short | long)

Parameter	Parameter Description	Parameter Value
short	Set LACP short timeout	-
long	Set LACP long timeout	-

Command Mode

Interface Configuration

Default

Long

Usage

None

Examples

This example shows how to configure the port timeout short for the Link Aggregation Control Protocol (LACP):

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lacp timeout short
```

This example shows how to return to the default setting:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no lacp timeout
```

Related Commands

None

3.6.6 lacp system-priority

Command Purpose

Use this command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the no form of this command to return to the default setting.

Command Syntax

lacp system-priority PRIORITY

Parameter	Parameter Description	Parameter Value
PRIORITY	LACP system priority	1-65535

Command Mode

Global Configuration

Default

32768

Usage

None

Examples

This example shows how to configure the system priority 100 for the Link Aggregation Control Protocol (LACP):

```
Switch# configure terminal
Switch(config)# lacp system-priority 100
```

This example shows how to return to the default setting:

```
Switch# configure terminal
Switch(config)# no lacp system-priority
```

Related Commands

None

3.6.7 port-channel channel-group-number load-balance-mode dynamic

Command Purpose

Use this command to enable dynamic load balance for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

port-channel GROUP_NUMBER load-balance-mode dynamic (flow-number FLOW_NUMBER |)

no port-channel GROUP_NUMBER load-balance-mode

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63
FLOW_NUMBER	Flow Number, default value is 32, can be 32/64/128/256	-

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable dynamic load balance for agg1:

```
Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode dynamic
```

Related Commands

None

3.6.8 port-channel channel-group-number load-balance-mode resilient**Command Purpose**

Use this command to enable resilient load balance for the Link Aggregation Group(both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

port-channel GROUP_NUMBER load-balance-mode resilient (flow-number FLOW_NUMBER |)

no port-channel channel-group-number load-balance-mode

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63
FLOW_NUMBER	Flow Number, default value is 32, can be 32/64/128/256	-

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable resilient load balance for agg1:

```
Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode resilient
```

Related Commands

None

3.6.9 port-channel channel-group-number load-balance-mode round-robin**Command Purpose**

Use this command to enable round-robin load balance for the Link Aggregation Group(both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

port-channel GROUP_NUMBER load-balance-mode dynamic

no port-channel GROUP_NUMBER load-balance-mode round-robin (flow-number FLOW_NUMBER |)

no port-channel GROUP_NUMBER load-balance-mode channel-group-number load-balance-mode

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63
FLOW_NUMBER	Flow Number, default value is 24	-

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable dynamic load balance for agg1:

```
Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode dynamic
```

Related Commands

None

3.6.10 port-channel channel-group-number self-healing**Command Purpose**

Use this command to enable self-healing for the Link Aggregation Group(both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

port-channel GROUP_NUMBER self-healing

no port-channel GROUP_NUMBER self-healing

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the self-healing, the Link Aggregation Group should not be create.

Examples

This example shows how to enable self-healing for agg1:

```
Switch# configure terminal
Switch(config)# port-channel 1 self-healing
```

Related Commands

None

3.6.11 port-channel channel-group-number static**Command Purpose**

Use this command to enable static load balance for the Link Aggregation Group (both static and dynamic aggregator). Use the no form of this command to return to the default setting.

Command Syntax

```
port-channel GROUP_NUMBER load-balance-mode static
no port-channel channel-group-number load-balance-mode
```

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63
FLOW_NUMBER	Flow Number, default value is 16, can be 1~24/32/64/128	-

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the load-balance mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable static load balance for agg1:

```
Switch# configure terminal
Switch(config)# port-channel 1 load-balance-mode static
```

Related Commands

None

3.6.12 port-channel channel-group-number lacp-mode dynamic**Command Purpose**

Use this command to enable dynamic lacp for the Link Aggregation Group (only dynamic aggregator). Use the no form of this command to unset the setting.

Command Syntax

port-channel GROUP_NUMBER lacp-mode dynamic

no port-channel GROUP_NUMBER lacp-mode

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Global Configuration

Default

None

Usage

Before enable or disable the dynamic lacp mode, the Link Aggregation Group should not be create.

Examples

This example shows how to enable dynamic lacp-mode for agg1:

```
NoneSwitch# configure terminal
Switch(config)# port-channel 1 lacp-mode dynamic
```

Related Commands

None

3.6.13 port-channel group-mode

Command Purpose

Use this command to switch the Link Aggregation Group mode. Use the no form of this command to return to the default group mode(56).

Command Syntax

port-channel group-mode (8 | 16 | 32 | 56)

no port-channel group-mode

Parameter	Parameter Description	Parameter Value
8	Group mode 8, the group range is 1~7	8
16	Group mode 16, the group range is 1~15	16
32	Group mode 32, the group range is 1~31	32
56	Group mode 32, the group range is 1~55	56

Command Mode

Global Configuration

Default

Flexible

Usage

The linkagg group-mode you specified will not take effect until you save configuration and reboot

Examples

This example shows how to switch to group mode 32:

```
Switch# configure terminal
Switch(config)# port-channel group-mode 32
```

Related Commands

None

3.6.14 show channel-group summary

Command Purpose

Use this command to display a summary of all of the channel groups, or a specified channel group.

Command Syntax

show channel-group (channel-group-number |) summary

Parameter	Parameter Description	Parameter Value
channel-group-number	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display a summary of all of the channel groups:

```
Switch# show channel-group summary
```

```
port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
    ipsa ipda srcport dstport ip-protocol
port-channel group-mode: flexible
```

```
Flags:  s - Suspend          T - Standby
        D - Down/Admin down  B - In bundle
        R - Layer3          S - Layer2
        w - Wait            U - In use
```

```
Mode:   SLB  - Static load balance
        DLB  - Dynamic load balance
        SHLB - Self-healing load balance
        RR   - Round robin load balance
```

Aggregator Name	Mode	Protocol	Ports
agg4(SD)	SLB	Static	eth-0-10(D)

Related Commands

None

3.6.15 show channel-group detail**Command Purpose**

Use this command to display detailed information of all of the channel groups, or a specified channel group.

Command Syntax

show channel-group (GROUP_NUMBER |) detail

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display detailed information of the channel group 10:

```
Switch# show channel-group detail
```

```
Channel-group listing:
```

```
-----
```

```
Group: 4
```

```
-----
```

```
Group state = L2
```

```
Ports: 1    Maxports : 16
```

```
Number of ports in bundle: 0 Max Channel-groups : 63
```

```
Protocol:   Static
```

```
Ports in the group:
```

```
-----
```

```
Port: eth-0-10
```

```
-----
```

```
Port state      : down Not-in-Bndl
```

```
Channel group : 4          Protocol : Static
```

```
Port-channel   : agg4
```

```
Port index     : 10
```

Related Commands

None

3.6.16 show lacp internal**Command Purpose**

Use this command to display internal information of all of the channel groups, or a specified channel group.

Command Syntax

show lacp (GROUP_NUMBER |) internal

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display internal information of all of the channel groups:

```
Switch# show lacp internal

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

Channel group 1

Port      LACP port Admin  Oper  Port  Port
Port      Flags State   Priority key   Key   Number State
eth-0-9   SA   bndl   32768  1     1     0x9   0x3d
```

Related Commands

None

3.6.17 show lacp internal detail

Command Purpose

Use this command to display detailed internal information of all of the channel groups, or a specified channel group.

Command Syntax

show lacp (GROUP_NUMBER |) internal detail

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display detailed internal information of all of the channel groups:

```
Switch# show lacp internal detail
```

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

Channel group 1

Actor's information:

Port	Actor System ID	Actor Port Number	Actor Flags
eth-0-9	32768,e0ef.1a32.7e00	0x9	SA

LACP Actor Port Priority	Actor Oper Key	Actor Port State
32768	1	0x4d

Port State Flags Decode:

Activity:	Timeout:	Aggregation:	Synchronization:
Active	Long	Yes	Yes

Collecting:	Distributing:	Defaulted:	Expired:
No	No	Yes	No

Related Commands

None

3.6.18 show lacp neighbor

Command Purpose

Use this command to display neighbor information of all of the channel groups, or a specified channel group.

Command Syntax

show lacp (GROUP_NUMBER |) neighbor

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display neighbor information of all of the channel groups:

Switch# show lacp neighbor

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

Channel group 1 neighbors

Partner's information:

Port	Flags	LACP port		Admin key	Oper Key	Port Number	Port State
		Priority	Dev ID				
eth-0-9	FP	0	0000.0000.0000	0	0	0x0	0x46

Related Commands

None

3.6.19 show lacp neighbor detail

Command Purpose

Use this command to display detailed neighbor information of all of the channel groups, or a specified channel group.

Command Syntax

show lacp (GROUP_NUMBER |) neighbor detail

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display detailed neighbor information of all of the channel groups:

```
Switch# show lacp neighbor detail
```

```
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
```

Channel group 1 neighbors

Partner's information:

Port	Partner System ID	Partner Port Number	Partner Flags
eth-0-9	32768,0000.0000.0000	0x0	SP

LACP Partner Port Priority	Partner Oper Key	Partner Port State
0	0	0x44

Port State Flags Decode:

Activity:	Timeout:	Aggregation:	Synchronization:
Passive	Long	Yes	No

Collecting:	Distributing:	Defaulted:	Expired:
No	No	Yes	No

Related Commands

None

3.6.20 show channel-group port

Command Purpose

Use this command to display details of the LACP port of all of the channel groups, or a specified channel group, or a specified port.

Command Syntax

show channel-group port (IFNAME |)

show channel-group GROUP_NUMBER port

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical ports
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display details of the LACP port of all of the channel group:

```
Switch# show channel-group port

Channel-group listing:
-----
Group: 1
-----
Ports in the group:
-----
Port: eth-0-9
-----

Port state      : Up Sngl-port-Bndl Not-in-Bndl
Channel number : 1          Protocol : LACP          Channel-group : agg1
Port index     : 9          Mode      : Active

Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
      A - Device is in active mode          P - Device is in passive mode

Local information:
Actor
Port  Flags  State  LACP port  Admin  Oper  Port  Port
eth-0-9 SA   indep  32768      1      1      9      0x4d

Partner's information:
Actor
Port  Flags  Priority  Dev ID      Oper  Port  Port
eth-0-9 SP   0        0000.0000.0000  0      0      0x44
```

This example shows how to display details of the LACP port of a specified port:

```
Switch# show channel-group port eth-0-9
```

```
Port: eth-0-9
```

```
-----
Port state      : Up Sngl-port-Bndl Not-in-Bndl
Channel number : 1          Protocol : LACP          Channel-group : agg1
Port index     : 9          Mode      : Active
```

```
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs
       A - Device is in active mode          P - Device is in passive mode
```

```
Local information:
```

Actor Port	Flags	State	LACP port Priority	Admin Key	Oper Key	Port Number	Port State
eth-0-9	SA	indep	32768	1	1	9	0x4d

```
Partner's information:
```

Actor Port	Flags	LACP port Priority	Dev ID	Oper Key	Port Number	Port State
eth-0-9	SP	0	0000.0000.0000	0	0	0x44

Related Commands

None

3.6.21 show lacp counters

Command Purpose

Use this command to display the packet traffic on all of the channel groups, or a specified channel group.

Command Syntax

```
show lacp [ GROUP_NUMBER ] counters
```

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the packet traffic on all of the channel groups:

```
Switch# show lacp counters
```

```
Traffic statistics
```

Port	LACPDUs		Pkts err	
	Sent	Recv	Sent	Recv
Channel-group agg1				
eth-0-9	27	0	0	0

Related Commands

None

3.6.22 show lacp sys-id

Command Purpose

Use this command to display the LACP system ID.

Command Syntax

```
show lacp sys-id
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the LACP system ID:

```
Switch# show lacp sys-id  
System ID: 32768,4600.0987.6c01
```

Related Commands

None

3.6.23 clear lacp counters

Command Purpose

Use this command to clear all counters of all of the channel groups, or a specified channel group.

Command Syntax

```
clear lacp ( GROUP_NUMBER | ) counters
```

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	0-63

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all counters of all of the channel groups:

```
Switch# clear lacp counters
```

This example shows how to clear a specified channel group:

```
Switch# clear lacp 10 counters
```

Related Commands

None

3.6.24 debug lacp

Command Purpose

Use this command to specify the options for the displayed debugging information for LACP cli, LACP event, LACP ha, LACP packet, LACP sync and LACP timer. Use the no parameter with this command to disable all debugging.

Command Syntax

debug lacp (all | cli | event | ha | packet | sync | timer)

no debug lacp (all | cli | event | ha | packet | sync | timer)

Parameter	Parameter Description	Parameter Value
all	All LACP debug information	-
cli	LACP commands debug information is displayed	-
event	LACP events debug information is displayed	-
ha	LACP high availability events debug information is displayed	-
packet	LACP packet contents debug information is displayed	-
sync	LACP synchronization debug information is displayed	-
timer(detail)	LACP timer expiry debug information is displayed	-

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

The following example displays information about the lacp packets that are received and sent out from the connected router:

```
Switch# debug lacp packet
```

Related Commands

show debugging lacp

3.6.25 show debugging lacp

Command Purpose

Use this command to display the LACP debugging status for these debugging options: LACP cli debugging, LACP event debugging, LACP ha debugging, LACP packet debugging, LACP sync debugging and LACP timer debugging.

Command Syntax

show debugging lacp

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show debugging lacp command:

```
Switch# show debugging lacp

LACP debugging status:
  LACP packet debugging is on
```

Related Commands

debug lacp all

3.7 VLAN Classification Commands

3.7.1 vlan classifier activate

Command Purpose

Use this command to apply vlan classifier group to an interface.

To remove it, use the no form of this command.

Command Syntax

vlan classifier activate GROUP_NUMBER based (ip | mac | protocol)

no vlan classifier activate

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	VLAN classifier group id	0-31, only group id 31 can be used for protocol
ip	Based on ip	-
mac	Based on MAC	-
protocol	Based on protocol	-

Command Mode

Interface Configuration

Default

None

Usage

An interface can only be applied by one vlan classifier group.

One vlan classifier group can apply more than one interface.

This command applies vlan classifier group to interface, and the interface can classify packets to different vlan according to the rule in vlan classifier group.

To create the rule, refer to vlan classifier rule command.

To create the group, refer to vlan classifier group command.

Examples

This example shows how to apply vlan classifier group 1 to the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# vlan classifier activate 1 based ip
```

This example shows how to remove the vlan classifier group 1 from the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no vlan classifier activate
```

Related Commands

vlan classifier group

vlan classifier rule

3.7.2 vlan classifier group

Command Purpose

Use this command to add or delete rule to vlan classifier group. Use the no form of this command to delete the group.

Command Syntax

vlan classifier group GROUP_NUMBER (add | delete) rule RULE

no vlan classifier group group

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	VLAN classifier group id	0-31, only group id 31 can be used for protocol
add	Add rule to vlan classifier group	-
delete	Delete rule to vlan classifier group	-
RULE	The id of rule	0-4095

Command Mode

Global Configuration

Default

None

Usage

To create the rule, refer to vlan classifier rule command.

To apply the vlan classifier group to an interface, refer to vlan classifier activate command.

When add a rule to the group by this command, the rule will be active immediately if the group has been applied to an interface already.

When delete a rule from the group by this command, the rule on this interface will be inactive immediately if the group is still applied to that interface.

The vlan classifier group will be deleted when the last rule on this group is deleted.

Examples

This example shows how to add rule1 to vlan classifier group 1:

```
Switch# configure terminal
Switch(config)# vlan classifier group 1 add rule 1
```

This example shows how to delete rule1 from vlan classifier group 1:

```
Switch# configure terminal
Switch(config)# vlan classifier group 1 delete rule 1
```

This example shows how to delete vlan classifier group 1:

```
Switch# configure terminal
Switch(config)# no vlan classifier group 1
```

Related Commands

vlan classifier activate

vlan classifier rule

3.7.3 vlan classifier rule

Command Purpose

Use this command to create vlan classifier rule.

To remove the vlan classifier rule, use the no form of this command.

Command Syntax

vlan classifier rule RULE (ip IP_ADDR | ipv6 IPV6_ADDR | mac MAC_ADDR | protocol (arp | ip | mpls | mpls-mcast | pppoe | rarp)) vlan VLAN_ID

no vlan classifier rule RULE

Parameter	Parameter Description	Parameter Value
RULE	The id of vlan classifier rule	0-4095
IP_ADDR	The source of ipv4 address in packets	IPv4 address
IPV6_ADDR	The source of ipv6 address in packets	IPv6 address
MAC_ADDR	The source of mac address in packets	Mac address in HHHH.HHHH.HHHH format
protocol	Specify an ethernet protocol classification	-
arp	Specify ARP protocol	-
ip	Specify IP protocol	-
mpls	Specify MPLS protocol	-
mpls-mcast	Specify MPLS multi cast protocol	-
pppoe	Specify PPPOE protocol	-
rarp	Specify RARP protocol	-
VLAN_ID	The vlan id to be assigned	1-4094

Command Mode

Global Configuration

Default

None

Usage

The rule will be effective only in inbound on interface.

The vlan id assigned by vlan classifier rule will be appended to the packets which match the rule.

To add this rule to vlan classifier group or apply the group to an interface, refer to vlan classifier group and vlan classifier activate command.

Examples

This example shows how to create rule1 which will classify all ipv4 packets to vlan11:

```
Switch# configure terminal
Switch(config)# vlan classifier rule 1 protocol ip vlan 11
```

This example shows how to delete rule1:

```
Switch# configure terminal
Switch(config)# no vlan classifier rule 1
```

Related Commands

vlan classifier group
vlan classifier activate

3.7.4 vlan classifier default-action**Command Purpose**

Use this command to set action when not hit vlan classifier rule. Use the no form of this command to restore default action.

Command Syntax

vlan classifier default-action drop
no vlan classifier default-action drop

Command Mode

Interface Configuration

Default

None

Usage

When packet input the port which enable vlan classifier and not hit any vlan classifier rule, the packet will be dropped.

Examples

This example shows how to set default action drop:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# vlan classifier default-action drop
```

This example shows how to set default action not drop:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no vlan classifier default-action drop
```

Related Commands

vlan classifier activate

3.7.5 show vlan classifier group**Command Purpose**

Use this command to show the information about vlan classifier group.

Command Syntax

show vlan classifier group GROUP_ID

Parameter	Parameter Description	Parameter Value
GROUP_ID	VLAN classifier group id	0-31, only group id 31 can be used for protocol

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display information about vlan classifier group 1:

```
Switch# show vlan classifier group 1
```

Related Commands

show vlan classifier interface

show vlan classifier rule

3.7.6 show vlan classifier interface**Command Purpose**

Use this command to show the information about vlan classifier group on interface.

Command Syntax

show vlan classifier interface group GROUP_ID

Parameter	Parameter Description	Parameter Value
GROUP_ID	VLAN classifier group id	0-31, only group id 31 can be used for protocol

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display information about vlan classifier group 1 on interface:

```
Switch# show vlan classifier interface group 1
```

Related Commands

show vlan classifier group

show vlan classifier rule

3.7.7 show vlan classifier rule**Command Purpose**

Use this command to show the information about vlan classifier rule.

Command Syntax

show vlan classifier rule (RULE |)

Parameter	Parameter Description	Parameter Value
RULE	The id of vlan classifier rule	0-4095

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display information about all the vlan classifier rules:

```
Switch# show vlan classifier rule
```

This example shows how to display information about the vlan classifier rule1:

```
Switch# show vlan classifier rule 1
```

Related Commands

show vlan classifier group

show vlan classifier interface

3.7.8 show resource vlan-classification

Command Purpose

Use this command to display the resource statistic used by vlan classification rules.

Command Syntax

show resource vlan-classification

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource vlan-classification command:

```
Switch# show resource vlan-classification
```

VLAN-CLASS

Resource	Used	Capability
MAC Based VLAN Classification	0	512
IPv4 Based VLAN Classification	0	512

Related Commands

None

3.8 VLAN Mapping Commands**3.8.1 ethernet evc****Command Purpose**

Use this command to add or delete EVC table.

Command Syntax

ethernet evc WORD

no ethernet evc WORD

Parameter	Parameter Description	Parameter Value
WORD	EVC name	Up to 16 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

Create ethernet evc evc_table:

```
Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-vlan 10
```

Related Commands

show ethernet evc NAME

3.8.2 dot1q mapped-vlan**Command Purpose**

Use this command to add evc entry to EVC table.

dot1q mapped-vlan VLAN_ID

no dot1q mapped-vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Mapped vlan id	1-4094

Command Mode

EVC Configuration

Default

None

Usage

None

Examples

Add EVC mapped-vlan entry, mapped vlan is 100:

```
Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-vlan 100
```

Related Commands

show ethernet evc NAME

3.8.3 dot1q mapped-double-vlan**Command Purpose**

Use this command to add evc entry with double vlans to EVC table.

Command Syntax

dot1q mapped-double-vlan INNER_VLAN_ID OUTER_VLAN_ID

no dot1q mapped-double-vlan

Parameter	Parameter Description	Parameter Value
INNER_VLAN_ID	Mapped inner vlan id	1-4094
OUTER_VLAN_ID	Mapped outer vlan id	1-4094

Command Mode

EVC Configuration

Default

None

Usage

This command is only used for untagged packet

Examples

Add EVC mapped-vlan entry, mapped inner vlan is 100, mapped outer vlan is 10:

```
Switch# configure terminal
Switch(config)# ethernet evc evc_table
Switch(config-evc)# dot1q mapped-double-vlan 100 10
```

Related Commands

show ethernet evc NAME

3.8.4 vlan mapping table

Command Purpose

Use this command to add or delete vlan mapping table.

Command Syntax

vlan mapping table WORD

no vlan mapping table WORD

Parameter	Parameter Description	Parameter Value
WORD	The name of vlan mapping table	Up to 16 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

Create vlan mapping table VMT:

```
Switch# configure terminal
Switch(config)# vlan mapping table VMT
Switch(config-vlan-mapping)#
```

Related Commands

show vlan mapping table WORD

3.8.5 raw vlan group

Command Purpose

Use this command to create raw VLAN group.

Command Syntax

raw vlan group GROUP_ID vlan VLAN_LIST

no raw vlan group GROUP_ID

Parameter	Parameter Description	Parameter Value
GROUP_ID	Raw vlan group id	1-64
VLAN_LIST	The VLAN ID list, example: 2-5,9-11	vlan list connected with '-' and ',' for example, "1-10,15,20,30-40"

Command Mode

Global Configuration

Default

None

Usage

None

Examples

Create raw VLAN group 1 and the VLAN list is from 10 to 20:

```
Switch# configure terminal
Switch(config)# raw vlan group 1 vlan 10-20
```

Related Commands

show vlan mapping table WORD

3.8.6 raw-vlan

Command Purpose

Use this command to add vlan mapping entry into vlan mapping table.

Command Syntax

raw-vlan (VLAN_ID | out-of-range | untagged | group GROUP_ID) evc WORD

no raw-vlan (VLAN_ID | out-of-range | untagged | group)

raw-vlan INNER_VLAN OUTER_VLAN egress-vlan (untagged | MAPPED_VLAN)

no raw-vlan INNER_VLAN OUTER_VLAN egress-vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Raw vlan id, range from 1~4094, the format could be 1,2,3 or 1-20.	vlan list connected with '-' and ',' for example, "1-10,15,20,30-40"
out-of-range	Vlan id isn't specified	-
untagged	Untagged packet	-
group GROUP_ID	Raw VLAN group, The group will use less resource compare with VLAN range.	1-64
WORD	EVC name	Up to 16 characters
INNER_VLAN	Inner vlan id	1-4094
OUTER_VLAN	Outer vlan id	1-4094
MAPPED_VLAN	Mapped vlan id	1-4094

Command Mode

VLAN Mapping Configuration

Default

None

Usage

None

Examples

Add vlan mapping entry, raw vlan is from 10 to 20, mapped evc is evc_table:

```
Switch# configure terminal
Switch(config)# vlan mapping table VMT
Switch(config-vlan-mapping)# raw-vlan 10-20 evc evc_table
```

Related Commands

show vlan mapping table WORD

3.8.7 dot1q ethertype

Command Purpose

Use this command to set ethertype on interface.

Command Syntax

dot1q ethertype VALUE

no dot1q ethertype

Parameter	Parameter Description	Parameter Value
VALUE	Specify The ethertype of VLAN tag.	The format is HEX, the default value is 0x8100

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

Set ethertype to 0x9100:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1q ethertype 9100
```

Related Commands

None

3.8.8 show vlan mapping table

Command Purpose

Use this command to display current **vlan mapping table**.

Command Syntax

show vlan mapping table (WORD |)

Parameter	Parameter Description	Parameter Value
WORD	The vlan mapping table to be displayed	Up to 16 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example show all vlan mapping table existed in system:

```
Switch# show vlan mapping table
```

Table Name	EVC Name	Mapped VLAN	Forward Interface	Raw VLAN
=====	=====	=====	=====	=====
VMT	evc_table	100	n/a	10-20
VMT_double	evc_double	10(100)	n/a	untagged
VMT_forward	evc_forward	20	eth-0-9	30

Related Commands

show vlan mapping table applied-interface

3.8.9 show vlan mapping table applied-interface**Command Purpose**

Use this command to display who is using the vlan mapping table of interface.

Command Syntax

show vlan mapping table applied-interface

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example show which interface used the vlan mapping table:

```
Switch# show vlan mapping table applied-interface
```

Table Name	Interface Name	Type
=====	=====	=====
VMT	eth-0-1	802.1Q-Tunnel

Related Commands

show vlan mapping table WORD

3.8.10 switchport mode**Command Purpose**

Use this command to configure switchport mode

Command Syntax

switchport mode (access | trunk | dot1q-tunnel)

no switchport dot1q-tunnel

Parameter	Parameter Description	Parameter Value
access	Configure this port to access port	-
trunk	Configure this port to trunk port	-
dot1q-tunnel	Configure this port to dot1q-tunnel port	-

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure a switchport to dot1q-tunnel port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode dot1q-tunnel
```

Related Commands

show interface switchport

3.8.11 switchport dot1q-tunnel type

Command Purpose

Use this command to configure dot1q-tunnel type.

Command Syntax

switchport dot1q-tunnel type (basic | selective)

Parameter	Parameter Description	Parameter Value
basic	Dot1q-tunnel basic type	-
selective	Dot1q-tunnel selective type	-

Command Mode

Interface Configuration

Default

basic type

Usage

None

Examples

This command is used to configure dot1q-tunnel type:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel type selective
```

Related Commands

show interface switchport

3.8.12 switchport dot1q-tunnel native

Command Purpose

Use this command to configure a switch-port's default vlan.

Command Syntax

switchport dot1q-tunnel native (vlan | inner-vlan) VLAN_ID

no switchport dot1q-tunnel native vlan

Parameter	Parameter Description	Parameter Value
vlan	VLAN that will be added	-
inner-vlan	Untagged inner VLAN	-
VLAN_ID	Vlan Id	1-4094

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

Configure the eth-0-1 to dot1q-tunnel and configure this port's native to vlan 10:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 100
Switch(config-vlan)# exit
Switch(config)# interface eth-0-23
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport dot1q-tunnel native vlan 100
```

Related Commands

None

3.8.13 switchport dot1q-tunnel allow vlan

Command Purpose

Use this command to configure dot1q-tunnel allowed vlan.

Command Syntax

switchport dot1q-tunnel allow vlan (all | none | add VLAN_ID | remove VLAN_ID)

Parameter	Parameter Description	Parameter Value
all	Add all VLANs to the allowed VLAN list	-
none	Remove all VLANs from the allowed VLAN list	-
add VLAN_ID	Add VLANs to the allowed VLAN list	1-4094
remove VLAN_ID	Remove VLANs from the allowed VLAN list	1-4094

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

Configure dot1q-tunnel allowed vlan 100 on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 100
```

Related Commands

show vlan brief

3.8.14 switchport dot1q-tunnel vlan mapping table

Command Purpose

Use this command to apply vlan mapping table on selective dot1q tunnel port.

Command Syntax

switchport dot1q-tunnel vlan mapping table WORD

no switchport dot1q-tunnel vlan mapping table

Parameter	Parameter Description	Parameter Value
WORD	VLAN mapping table name	Up to 16 characters

Command Mode

Interface Configuration

Default

None

Usage

Apply exist vlan mapping table on dot1q-tunnel port. The type of dot1q-tunnel port should be selective.

Examples

The following is a sample that applying vlan mapping table on selective dot1q tunnel port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel vlan mapping table mp
```

Related Commands

show interface switchport

3.8.15 switchport dot1q-tunnel vlan mapping miss-forward

Command Purpose

Use this command to set packet do normal forward when vlan mapping table is not matched on selective dot1q tunnel port.

Command Syntax

switchport dot1q-tunnel vlan mapping miss-forward

no switchport dot1q-tunnel vlan mapping miss-forward

Command Mode

Interface Configuration

Default

None

Usage

Need to switch the dot1q-tunnel port in selective type before config this command.

Examples

The following is a sample that set packet do normal forward when vlan mapping table is not matched on selective dot1q tunnel port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport dot1q-tunnel vlan mapping miss-forward
```

Related Commands

3.8.16 switchport trunk vlan-translation

Command Purpose

Use this command to enable vlan translation.

Command Syntax

switchport trunk vlan-translation

no switchport trunk vlan-translation

Command Mode

Interface Configuration

Default

None

Usage

Use this command to enable vlan translation on trunk port. Only trunk port can enable vlan translation.

Examples

The following is a sample that enabling vlan translation on trunk port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk vlan-translation
```

Related Commands

show interface switchport

3.8.17 switchport trunk vlan-translation mapping table

Command Purpose

Use this command to apply vlan mapping table on vlan translation port.

Command Syntax

switchport trunk vlan-translation mapping table WORD

no switchport trunk vlan-translation mapping table

Parameter	Parameter Description	Parameter Value
WORD	VLAN mapping table name	Up to 16 characters

Command Mode

Interface Configuration

Default

None

Usage

Use this command to apply vlan mapping on vlan translation port.

Examples

The following is a sample that applying vlan mapping on vlan translation port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk vlan-translation vlan mapping table map_table
```

Related Commands

show interface switchport

3.8.18 switchport trunk vlan-translation miss-forward

Command Purpose

Use this command to allow the packet which not match vlan mapping table forward

Command Syntax

switchport trunk vlan-translation mapping miss-forward

no switchport trunk vlan-translation mapping miss-forward

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following is a sample that let the packet which not matched vlan mapping table forward:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport trunk vlan-translation mapping miss-forward
```

Related Commands

None

3.8.19 vlan dot1q tag native

Command Purpose

Use this command to set tag the vlan on packet if in default vlan

Command Syntax

vlan dot1q tag native

no vlan dot1q tag native

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following is a sample that tag the vlan if in default vlan:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# vlan dot1q tag native
```

Related Commands

None

3.8.20 show resource vlan-mapping

Command Purpose

Use this command to display the resource statistic used by vlan mapping table.

Command Syntax

show resource vlan-mapping

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource vlan-mapping command:

```
Switch# show resource vlan-mapping

VLAN-MAPPING
Resource                Used      Capability
=====
Applied VLAN Mapping Entry  0        1024
```

Related Commands

None

3.9 MSTP Commands

3.9.1 spanning-tree enable

Command Purpose

Use this command to enable the Spanning Tree Protocol on a bridge. Use the no parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax

spanning-tree enable

no spanning-tree enable

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to global enable stp:

```
Switch# configure terminal
Switch(config)# spanning-tree enable
```

This example shows how to global disable stp:

```
Switch# configure terminal
Switch(config)# no spanning-tree enable
```

Related Commands

show spanning-tree

3.9.2 spanning-tree priority

Command Purpose

Use this command to set the bridge priority for the common instance for the default bridge. Using a lower priority indicates a higher likelihood of the bridge becoming root. Use the no parameter with this command to reset it to the default value.

Command Syntax

spanning-tree priority PRIORITY

no spanning-tree priority

Parameter	Parameter Description	Parameter Value
PRIORITY	Bridge priority	0-61440

Command Mode

Global Configuration

Default

The default priority is 32678 (or hex 0x8000)

Usage

This command is used to set the priority of the bridge. The priority values must be in multiples of 4096.

Examples

This example shows how to set the bridge priority.:

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
```

This example shows how to reset the bridge priority to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree priority
```

Related Commands

show spanning-tree

3.9.3 spanning-tree instance priority

Command Purpose

Use this command to set the default bridge priority for an MST instance to the value specified. Use the no parameter with this command to restore the default value of the default bridge priority.

Command Syntax

spanning-tree instance INSTANCE_ID priority PRIORITY

no spanning-tree instance INSTANCE_ID priority

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the instance ID	1-4094
PRIORITY	Specify the bridge priority	0-61440

Command Mode

Global Configuration

Default

The default value of port priority for each instance is 32768.

Usage

The lower the priority of the bridge, there is higher likelihood that the bridge becomes a root bridge or a designated bridge for the LAN. The permitted range of values is 0-61440. The priority values must be in multiples of 4096.

Examples

This example shows how to set the priority for instance 1:

```
Switch# configure terminal
Switch(config)# spanning-tree instance 1 priority 0
```

Related Commands

show spanning-tree

3.9.4 spanning-tree forward-time

Command Purpose

Use this command to set the time after which (if this bridge is the root bridge) each port in the default bridge changes states to learning and forwarding. This value is used by all instances. Use the no parameter with this command to restore the default value of 15 seconds.

Command Syntax

spanning-tree forward-time SECONDS

no spanning-tree forward-time

Parameter	Parameter Description	Parameter Value
SECONDS	Forwarding time delay, in seconds, for the default bridge	2018/4/30

Command Mode

Global Configuration

Default

The default value is 15 seconds

Usage

The allowable range for the forward time is 4-30 seconds. It is not advisable to set the value below 7 seconds.

Examples

This example shows how to set the forward time to 16 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree forward-time 16
```

This example shows how to reset the forward time to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree forward-time
```

Related Commands

show spanning-tree

3.9.5 spanning-tree hello-time**Command Purpose**

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the default bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances.

Command Syntax

spanning-tree hello-time SECONDS

no spanning-tree hello-time

Parameter	Parameter Description	Parameter Value
SECONDS	Hello BPDU interval	1-10, unit:second

Command Mode

Global Configuration

Default

The default hello-time value is 2

Usage

The allowable range of values is 1-10 seconds.

Examples

This example shows how to set the hello time to 5 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 5
```

This example shows how to reset the hello-time to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree hello-time
```

Related Commands

show spanning-tree

3.9.6 spanning-tree max-age**Command Purpose**

Use this command to set the maximum age for the default bridge. Use the no parameter with this command to restore the default value of the maximum age.

Command Syntax

spanning-tree max-age SECONDS

no spanning-tree max-age

Parameter	Parameter Description	Parameter Value
SECONDS	The maximum time, in seconds, to listen for the root bridge	6-40

Command Mode

Global Configuration

Default

The default value of bridge maximum age is 20 seconds.

Usage

Maximum age is the maximum time for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, and less than twice the value of forward delay minus 1. The allowable range for maximum age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Examples

This example shows how to set the max age to 12 seconds:

```
Switch# configure terminal
Switch(config)# spanning-tree max-age 12
```

This example shows how to reset the max age to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree max-age
```

Related Commands

show spanning-tree

3.9.7 spanning-tree max-hops

Command Purpose

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. To restore the default value, use the no parameter with this command.

Command Syntax

spanning-tree max-hops NUMBER

no spanning-tree max-hops

Parameter	Parameter Description	Parameter Value
NUMBER	Max hops	1-40

Command Mode

Global Configuration

Default

The default maximum hops in an MST region are 20

Usage

Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU packets.

The configuration should be shown when the bridge is MSTP mode.

Examples

This example shows how to set the max hops to 25:

```
Switch# configure terminal
Switch(config)# spanning-tree max-hops 25
```

This example shows how to reset the max hops to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree max-hops
```

Related Commands

show spanning-tree

3.9.8 spanning-tree transmit-holdcount

Command Purpose

Use this command to set the maximum number of transmissions of BPDUs in an MST region by the transmit state machine. Use the no parameter with this command to restore the default transmit hold-count value.

Command Syntax

spanning-tree transmit-holdcount NUMBER

no spanning-tree transmit-holdcount

Parameter	Parameter Description	Parameter Value
NUMBER	Transmit hold-count value	1-10

Command Mode

Global Configuration

Default

Transmit hold-count default value is 3

Usage

None

Examples

This example shows how to set hold count to 5:

```
Switch# configure terminal
Switch(config)# spanning-tree transmit-holdcount 5
```

This example shows how to reset the hold count to default value:

```
Switch# configure terminal
Switch(config)# no spanning-tree transmit-holdcount
```

Related Commands

show spanning-tree

3.9.9 spanning-tree edgeport bpdu-guard

Command Purpose

Use this command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the no parameter with this command to disable the BPDU Guard feature on a bridge.

Command Syntax

spanning-tree edgeport bpdu-guard

no spanning-tree edgeport bpdu-guard

Command Mode

Global Configuration

Default

BPDU guard is disabled

Usage

Use the show spanning-tree command to display the bridge and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of the BPDU guard.

Examples

This example shows how to global enable bpdu-guard and enable bpdu-guard on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-guard enable
```

Related Commands

show spanning-tree interface

3.9.10 spanning-tree edgeport bpdu-filter

Command Purpose

Use this command to enable the edgeport BPDU filter for the bridge. Use the no parameter with this command to disable the BPDU filter for the bridge.

Command Syntax

```
spanning-tree edgeport bpdu-filter
no spanning-tree edgeport bpdu-filter
```

Command Mode

Global Configuration

Default

None

Usage

Use the show spanning tree command to display administratively configured, and currently running values, of the BPDU filter parameter for the bridge and port.

If bpdu-guard and bpdu-filter are all configed on port, bpdu-filter has a higher priority.

Examples

This example shows how to global enable bpdu-filter and enable bpdu-filter on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-filter
```

Related Commands

show spanning-tree interface

3.9.11 spanning-tree port

Command Purpose

Use this command to enable or disable spanning tree protocol on specified port.

Command Syntax

```
spanning-tree port ( enable | disable )
```

Parameter	Parameter Description	Parameter Value
enable	Enable spanning protocol on this port	-
disable	Disable spanning protocol on this port	-

Command Mode

Interface Configuration

Default

The default spanning tree state of the port is enabled.

Usage

None

Examples

This example shows how to enable STP on port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree port enable
```

This example shows how to disable STP on port eth-0-1:

```
Switch# configure terminal
Switch(config-if)# spanning-tree port disable
```

Related Commands

show spanning-tree interface

3.9.12 spanning-tree port-priority**Command Purpose**

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax

spanning-tree port-priority PRIORITY

no spanning-tree port-priority

Parameter	Parameter Description	Parameter Value
PRIORITY	Port priority	0-240

Command Mode

Interface Configuration

Default

The default priority is 128

Usage

None

Examples

This example shows how to set the priority to 240 on port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree port-priority 240
```

Related Commands

show spanning-tree interface

3.9.13 spanning-tree pathcost-standard**Command Purpose**

Use this command to set the path cost standard associated with the default bridge-group. Use the no parameter with this command to set to default value.

Command Syntax

spanning-tree pathcost-standard (dot1d-1998 | dot1t)

no spanning-tree pathcost-standard

Parameter	Parameter Description	Parameter Value
dot1d-1998	IEEE 802.1D-1998 standard	-
dot1t	IEEE 802.1T standard	-

Command Mode

Global Configuration

Default

The default pathcost-standard is dot1t

Usage

If the pathcost-standard is changed, cost of every port will be reset and auto-calculated.

Examples

This example shows how to set the path cost standard:

```
Switch# configure terminal
Switch(config)# spanning-tree pathcost-standard dot1d-1998
```

Cost of every port has been reset and auto-calculation is available

Related Commands

show spanning-tree

3.9.14 spanning-tree path-cost

Command Purpose

Use this command to set the cost of a path associated with the default bridge-group. The lower the path cost, the greater likelihood of the bridge becoming root. Use the no parameter with this command to calculate path cost according to interface's speed.

Command Syntax

spanning-tree path-cost NUMBER

no spanning-tree path-cost

Parameter	Parameter Description	Parameter Value
NUMBER	The cost to be assigned to the group.	The range is 1 to 200000000 for dot1t and 1-65535 for dot1d-1998

Command Mode

Interface Configuration

Default

The default path cost value is calculated according to interface's speed

Usage

None

Examples

This example shows how to set the STP path-cost to 123:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree path-cost 123
```

This example shows how to reset the STP path-cost to default value:

```
Switch# configure terminal
Switch(config-if)# no spanning-tree path-cost
```

Related Commands

show spanning-tree interface

3.9.15 spanning-tree link-type**Command Purpose**

Use this command to enable or disable point-to-point or shared link types. Use the no parameter with this command to disable rapid transition.

Command Syntax

spanning-tree link-type (auto | point-to-point | shared)

no spanning-tree link-type

Parameter	Parameter Description	Parameter Value
auto	Automatically detect link type	-
point-to-point	Enable point to point link	-
shared	Disable point to point link	-

Command Mode

Interface Configuration

Default

The link type is auto detected

Usage

None

Examples

This example shows how to set the link type to shared on port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree link-type shared
```

Related Commands

show spanning-tree brief

3.9.16 spanning-tree edgeport**Command Purpose**

Use this command to set a port as an edge-port and to enable rapid transitions. Use the no parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Command Syntax

spanning-tree edgeport

no spanning-tree edgeport

Command Mode

Interface Configuration

Default

The port is not an edge-port

Usage

None

Examples

This example shows how to set the port eth-0-1 to edgeport:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
```

This example shows how to reset the port to an non-edgeport:

```
Switch# configure terminal
Switch(config-if)# no spanning-tree edgeport
```

Related Commands

show spanning-tree interface

3.9.17 spanning-tree edgeport bpdu-guard

Command Purpose

Use this command to enable or disable the BPDU Guard feature on a port. Use the no parameter with this command to set the BPDU Guard feature on a port to default.

Command Syntax

spanning-tree edgeport bpdu-guard (enable | disable | default)

no spanning-tree edgeport bpdu-guard

Parameter	Parameter Description	Parameter Value
enable	Enable edgeport bpdu-guard	-
disable	Disable edgeport bpdu-guard	-
default	Default	-

Command Mode

Interface Configuration

Default

BPDU guard is disabled on port

Usage

None

Examples

This example shows how to change port to edgeport and enable bpdu-guard on port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-guard enable
```

Related Commands

show spanning tree interface

3.9.18 spanning-tree edgeport bpdu-filter

Command Purpose

Use this command to set edgeport BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to default.

Command Syntax

spanning-tree edgeport bpdu-filter (enable | disable | default)

no spanning-tree edgeport bpdu-filter

Parameter	Parameter Description	Parameter Value
enable	Enable edgeport bpdu-filter	-
disable	Disable edgeport bpdu-filter	-
default	Default	-

Command Mode

Interface Configuration

Default

BPDU filter is disabled on port

Usage

None

Examples

This example shows how to enable bpdu-filter on port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree edgeport
Switch(config-if)# spanning-tree edgeport bpdu-filter
```

This example shows how to disable bpdu-filter on port:

```
Switch# configure terminal
Switch(config-if)# no spanning-tree edgeport bpdu-filter
```

Related Commands

show spanning tree interface

3.9.19 spanning-tree guard root

Command Purpose

Use this command to enable the Root Guard feature for the port. This feature disables reception of superior BPDUs. Use the no parameter with this command to disable the root guard feature for the port.

Command Syntax

spanning-tree guard root

no spanning-tree guard root

Command Mode

Interface Configuration

Default

Root guard is disabled

Usage

The Root Guard feature makes sure that the port on which it is enabled is a designated port. If a port with Root Guard enabled receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Examples

This example shows how to enable the Root Guard feature for the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard root
```

This example shows how to disable the Root Guard feature for the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree guard root
```

Related Commands

None

3.9.20 spanning-tree guard loop

Command Purpose

Use this command to enable the loop guard feature for the port. This feature provides additional protection against Layer 2 forwarding loops. Use the no parameter with this command to disable the loop guard feature for the port.

Command Syntax

spanning-tree guard loop

no spanning-tree guard loop

Command Mode

Interface Configuration

Default

Loop guard is disabled

Usage

The loop guard feature should be enabled on the non-designated ports. When a port enables loop guard, and BPDUs are not received on a non-designated port after max_age, the port should move into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state, and should not pass user traffic.

Examples

This example shows how to enable the loop guard on the port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree guard loop
```

Related Commands

spanning-tree guard root

3.9.21 spanning-tree force-version

Command Purpose

Use this command to specify the version. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-3, for RSTP, the valid range is 0-2. Use the no parameter with this command to set the default protocol version.

Command Syntax

spanning-tree force-version NUMBER

no spanning-tree force-version

Parameter	Parameter Description	Parameter Value
NUMBER	Version identifier.	0 - STP, 1- Not supported, 2 - RSTP, 3 - MSTP

Command Mode

Interface Configuration

Default

STP default 0, RSTP default 2, MSTP default 3

Usage

None

Examples

This example shows how to specify the version:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree force-version 1
```

This example shows how to reset the default version:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree force-version
```

Related Commands

None

3.9.22 spanning-tree restricted-tcn**Command Purpose**

Use this command to set the restricted TCN value of the port to TRUE. Use the no parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax

spanning-tree restricted-tcn
no spanning-tree restricted-tcn

Command Mode

Interface Configuration

Default

The default restricted TCN value is FALSE

Usage

None

Examples

This example shows how to set the restricted TCN value of the port to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-tcn
```

This example shows how to set the restricted TCN value of the port to FALSE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree restricted-tcn
```

Related Commands

None

3.9.23 spanning-tree restricted-role

Command Purpose

Use this command to set the restricted-role value of the port to TRUE. Use the no parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax

spanning-tree restricted-role

no spanning-tree restricted-role

Command Mode

Interface Configuration

Default

The default restricted-role value is FALSE

Usage

None

Examples

This example shows how to set the restricted-role value of the port to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree restricted-role
```

This example shows how to set the restricted-role value of the port to FALSE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree restricted-role
```

Related Commands

None

3.9.24 spanning-tree tc-protection

Command Purpose

Use this command to set the tc-protection value to TRUE. Use the no parameter with this command to set the tc-protection value to FALSE. If tc-protection is set, the number of tc packets which can be processed every hello time interval shouldn't be greater than the number of tc-protection threshold.

Command Syntax

spanning-tree tc-protection

no spanning-tree tc-protection

Command Mode

Global Configuration

Default

The default tc-protection value is FALSE

Usage

None

Examples

This example shows how to set the tc-protection value to TRUE:

```
Switch# configure terminal
Switch(config)# spanning-tree tc-protection
```

This example shows how to set the tc-protection value to FALSE:

```
Switch# configure terminal
Switch(config)# no spanning-tree tc-protection
```

Related Commands

None

3.9.25 spanning-tree tc-protection threshold

Command Purpose

Use this command to set the tc-protection threshold value. Use the no parameter with this command to set the tc-protection threshold value to 1. If tc-protection is set, the number of tc packets which can be processed every hello time interval shouldn't be greater than the number of tc-protection threshold.

Command Syntax

spanning-tree tc-protection threshold NUMBER

no spanning-tree tc-protection threshold

Parameter	Parameter Description	Parameter Value
NUMBER	Tc-protection threshold value, default 1	1-255

Command Mode

Global Configuration

Default

The default tc-protection threshold value is 1

Usage

None

Examples

This example shows how to set the tc-protection to 255:

```
Switch# configure terminal
Switch(config)# spanning-tree tc-protection threshold 255
```

This example shows how to reset the tc-protection to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree tc-protection threshold
```

Related Commands

None

3.9.26 spanning-tree mode

Command Purpose

Use this command to set spanning tree mode.

Command Syntax

spanning-tree mode (stp | rstp | mstp)

Parameter	Parameter Description	Parameter Value
stp	spanning tree protocol	-

Parameter	Parameter Description	Parameter Value
rstp	rapid spanning tree protocol	-
mstp	multiple spanning tree protocol	-

Command Mode

Global Configuration

Default

The default spanning-tree mode is stp

Usage

None

Examples

This example shows how to set the spanning tree mode to mstp:

```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
```

Related Commands

None

3.9.27 spanning-tree instance port-priority

Command Purpose

Use this command to set the port priority for a bridge group. Use the no parameter with this command to restore the default priority value.

Command Syntax

spanning-tree instance INSTANCE_ID port-priority PRIORITY

no spanning-tree instance INSTANCE_ID port-priority

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the identifier	1-4094
PRIORITY	Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The range is 0~240	0-240

Command Mode

Interface Configuration

Default

The default priority is 128

Usage

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frame for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

The permitted range is 0-240. The priority values can only be set in increments of 16.

Examples

This example shows how to set the port priority to 112 for instance 3:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 3 port-priority 112
```

This example shows how to reset the port priority to default value for instance 3:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no spanning-tree instance 3 port-priority
```

Related Commands

None

3.9.28 spanning-tree instance path-cost

Command Purpose

Use this command to set the cost of a path associated with an interface. Use the no parameter with this command to restore the default cost value of the path.

Command Syntax

```
spanning-tree instance INSTANCE_ID path-cost COST
```

```
no spanning-tree instance INSTANCE_ID path-cost
```

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the identifier	1-4094
COST	Specify the cost of path	<1-200000000> for dot1t and <1-65535> for dot1d-1998 (a lower path-cost indicates a greater likelihood of the specified interface becoming a root)

Command Mode

Interface Configuration

Default

Assuming a 10 Mb/s link speed, the default value is configured as 2,000,000

Usage

Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the bridge-group instance command (see the example below).

Examples

This example shows how to set the cost of a path associated with an interface:

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 3 vlan 3
Switch(config-mst)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 3
Switch(config-if)# spanning-tree instance 3 path-cost 1000
Switch(config-mst)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# spanning-tree instance 3 path-cost 1000
```

Related Commands

None

3.9.29 spanning-tree instance restricted-tcn

Command Purpose

Use this command to set the restricted TCN value for the instance to TRUE. Use the no parameter with this command to set the restricted TCN value for the instance to FALSE.

Command Syntax

spanning-tree instance INSTANCE_ID restricted-tcn

no spanning-tree instance INSTANCE_ID restricted-tcn

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the instance ID	1-4094

Command Mode

Interface Configuration

Default

The default restricted TCN value is FALSE

Usage

None

Examples

This example shows how to set the restricted TCN value for the instance to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 2 restricted-tcn
```

Related Commands

None

3.9.30 spanning-tree instance restricted-role

Command Purpose

Use this command to set the restricted role value for the instance to TRUE. Use the no parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax

spanning-tree instance INSTANCE_ID restricted-role

no spanning-tree instance INSTANCE_ID restricted-role

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the instance ID	1-4094

Command Mode

Interface Configuration

Default

The default restricted-role value is FALSE.

Usage

None

Examples

This example shows how to set the restricted role value for the instance to TRUE:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 2 restricted-role
```

Related Commands

None

3.9.31 spanning-tree mst configuration

Command Purpose

Use this command to enter mst configuration mode.

Command Syntax

spanning-tree mst configuraiton

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to enter into mst configuration mode:

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
```

Related Commands

None

3.9.32 instance

Command Purpose

Use this command to create an mstp instance and map VLANs to an MST instance.

Command Syntax

instance INSTANCE_ID vlan VLAN_ID

no instance INSTANCE_ID vlan VLAN_ID

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Instance id, we support at most 64 instances	1-4094
VLAN_ID	The vlan associated with instance must be created first.	1-4094

Command Mode

MST Configuration

Default

None

Usage

When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped.

Examples

This example shows how to map vlan 10 to instance 1:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree Mst configuration
Switch(config-mst)# instance 1 vlan 10
```

Related Commands

None

3.9.33 region

Command Purpose

Use this command to create mstp region.

Command Syntax

region NAME

no region NAME

Parameter	Parameter Description	Parameter Value
NAME	Specify the region name	The name string has a maximum length of 32 characters and is case sensitive

Command Mode

MST Configuration

Default

The default region name is an empty string

Usage

None

Examples

This example shows how to set the region to Switch :

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 10
Switch(config-vlan)# exit
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# region Switch
```

Related Commands

None

3.9.34 revision

Command Purpose

Use this command to create an mstp revision number.

Command Syntax

revision NUMBER

no revision NUMBER

Parameter	Parameter Description	Parameter Value
NUMBER	Specify the configuration revision number	0-65535

Command Mode

MST Configuration

Default

Default value is 0

Usage

None

Examples

This example shows how to set the revision number to 1:

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 1
```

Related Commands

None

3.9.35 clear spanning-tree detected protocols

Command Purpose

Use this command to clear the detected protocols for a specific bridge or interface.

Command Syntax

clear spanning-tree detected protocols (interface IFNAME |)

Parameter	Parameter Description	Parameter Value
interface IFNAME	Specify the name of the interface on which protocols have to be cleared	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear the detected protocols for a specific bridge or interface eth-0-1:

```
Switch# clear spanning-tree detected protocols interface eth-0-1
```

Related Commands

None

3.9.36 clear spanning-tree disabled-port

Command Purpose

Use this command to clear all spanning tree protocol disabled port.

Command Syntax

clear spanning-tree disabled-port

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all spanning tree protocol disabled port:

```
Switch# clear spanning-tree disabled-port
```

Related Commands

None

3.9.37 show spanning-tree

Command Purpose

Use this command to show the state of the spanning tree. This command only shows up interface's state.

Command Syntax

show spanning-tree

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the state of spanning tree:

```
Switch# show spanning-tree

  Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
```

```

eth-0-1: Designated External Path Cost 0 - Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 373 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point

```

Related Commands

None

3.9.38 show spanning-tree interface

Command Purpose

Use this command to show the state of the spanning tree of the specified interface.

Command Syntax

show spanning-tree interface IFNAME (brief |)

Parameter	Parameter Description	Parameter Value
IFNAME	Specify the name of the interface	-
brief	The brief spanning-tree information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the state of the spanning tree of the interface eth-0-1:

```

Switch# show spanning-tree interface eth-0-1

Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00

```



```

CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change t
imer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 352 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
eth-0-1: Edgeport bpdu-guard Default - Current edgeport bpdu-guard off
eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
eth-0-1: No root guard configured - Current root guard off
eth-0-1: No loop guard configured - Current loop guard off
eth-0-1: Configured Link Type auto - Current point-to-point

```

Related Commands

None

3.9.39 show spanning-tree brief

Command Purpose

Use this command to show the brief state of the spanning tree.

Command Syntax

show spanning-tree brief

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the brief state of the spanning tree The down interface should not be show:

```

Switch# show spanning-tree brief

Multiple spanning tree protocol Enabled
Root ID      Priority    32768 (0x8000)
              Address      8afa.58e9.cb00
              Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
Bridge ID    Priority    32768 (0x8000)
              Address      8afa.58e9.cb00
              Hello Time  2 sec  Max Age  20 sec Forward Delay 15 sec
              Aging Time  300 sec

```

Interface	Role	State	Cost	Priority.Number	Type
eth-0-1	Designated	Forwarding	20000	128.1	P2p
eth-0-2	Designated	Forwarding	20000	128.2	P2p

Related Commands

None

3.9.40 show spanning-tree disabled-port**Command Purpose**

Use this command to show the spanning tree protocol disabled port.

Command Syntax

show spanning-tree disabled-port

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying all spanning tree protocol disabled port:

```
Switch# show spanning-tree disabled-port
```

```
Interface
```

```
-----  
eth-0-1
```

Related Commands

None

3.9.41 show spanning-tree mst**Command Purpose**

Use this command to show the mstp information.

Command Syntax

show spanning-tree mst

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the mstp information The down interface should not be show:

```
Switch#show spanning-tree mst
```

```

Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
Instance  Interface  VLAN
0 :                1, 3
1 :      eth-0-2    2

```

Related Commands

None

3.9.42 show spanning-tree mst config

Command Purpose

Use this command to show the mstp region configuration information.

Command Syntax

show spanning-tree mst config

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the mstp region configuration information:

```
Switch#show spanning-tree mst config
```

MSTP Configuration Information:

```

-----
Format Id      : 0
Name           : switch
Revision Level : 0
Digest         : 0x3AB68794D602FDF43B21C0B37AC3BCA8
Instances configured 1
-----

```

Instance Vlans mapped

```

-----
0          1, 3
1          2
-----

```

Related Commands

None

3.9.43 show spanning-tree mst detail

Command Purpose

Use this command to show the detail mstp information.

Command Syntax

show spanning-tree mst detail (interface IFNAME |)

Parameter	Parameter Description	Parameter Value
interface IFNAME	The interface name you want to display	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the mstp information The down interface should not be show:

```
Switch#show spanning-tree mst detail interface eth-0-1

Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 80008afa58e9cb00
CIST Reg Root Id 80008afa58e9cb00
CIST Bridge Id 80008afa58e9cb00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
eth-0-1: Designated Port Id 8001 - CIST Priority 128
eth-0-1: CIST Root 80008afa58e9cb00
eth-0-1: Regional Root 80008afa58e9cb00
eth-0-1: Designated Bridge 80008afa58e9cb00
eth-0-1: Message Age 0 - Max Age 20
eth-0-1: CIST Hello Time 2 - Forward Delay 15
eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
eth-0-1: Forward-transitions 2
eth-0-1: BPDU sent 247 - BPDU received 0
eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
eth-0-1: No edgeport configured - Current edgeport off
```

Related Commands

None

3.9.44 show spanning-tree mst instance

Command Purpose

Use this command to show the detail mstp information of a specific instance.

Command Syntax

show spanning-tree mst instance INSTANCE_ID (interface IFNAME |)

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Instance number you want to display	1-4094
IFNAME	The interface name you want to display	Support physical/aggregation ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the detail mstp information:

```
Switch#show spanning-tree mst instance 2
```

```
MSTI Root Path Cost 0 - MSTI Root Port 0
MSTI Root Id 8002e083bce89601
MSTI Bridge Id 8002e083bce89601
MSTI Bridge Priority 32768

eth-0-48: Port 48 - Id 8030 - Role Disabled - State Discarding
eth-0-48: Designated Internal Path Cost 0 - Designated Port Id 0
eth-0-48: Configured Internal Path Cost 20000
eth-0-48: Configured CST External Path cost 20000
eth-0-48: CST Priority 128 - MSTI Priority 128
eth-0-48: Designated Root 0000000000000000
eth-0-48: Designated Bridge 0000000000000000
eth-0-48: Message Age 0 - Max Age 0
eth-0-48: Hello Time 2 - Forward Delay 15
eth-0-48: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

eth-0-1: Port 1 - Id 8001 - Role Disabled - State Discarding
eth-0-1: Designated Internal Path Cost 0 - Designated Port Id 0
eth-0-1: Configured Internal Path Cost 20000
eth-0-1: Configured CST External Path cost 20000
eth-0-1: CST Priority 128 - MSTI Priority 128
eth-0-1: Designated Root 0000e083bce89601
eth-0-1: Designated Bridge 0000e083bce89601
eth-0-1: Message Age 0 - Max Age 0
eth-0-1: Hello Time 2 - Forward Delay 15
eth-0-1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

Related Commands

None

3.9.45 show spanning-tree mst interface

Command Purpose

Use this command to show the detail mstp information of a specific interface.

Command Syntax

show spanning-tree mst interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name you want to display	Support physical/aggregation ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the mstp information of an interface:

```
Switch# show spanning-tree mst interface eth-0-1

Bridge up - Spanning Tree Enabled
Mode - Multiple spanning tree protocol
Path Cost Standard - dot1t
CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
Tx Hold Count 6
CIST Root Id 8000be8c722f7f00
CIST Reg Root Id 8000be8c722f7f00
CIST Bridge Id 8000be8c722f7f00
Edgeport bpdu-filter disabled
Edgeport bpdu-guard disabled
Loop guard configured disabled
Instance  Interface  VLAN
0          eth-0-1    1, 4-100
1          eth-0-1    2
2          eth-0-1    3
```

Related Commands

None

3.9.46 show spanning-tree mst brief

Command Purpose

Use this command to show the brief mstp information.

Command Syntax

show spanning-tree mst brief (interface IFNAME | instance INSTANCE_ID |)

Parameter	Parameter Description	Parameter Value
interface IFNAME	The interface name you want to display	-
instance INSTANCE_ID	Instance number you want to display	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is an output of this command displaying the brief mstp information:

```
Switch#show spanning-tree mst brief

##### MST0: Vlan: 1
Multiple spanning tree protocol Enabled
Root ID      Priority    32768 (0x8000)
              Address    e083.bce8.9601
              Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec
Bridge ID    Priority    32768 (0x8000)
              Address    e083.bce8.9601
              Hello Time 2 sec   Max Age 20 sec Forward Delay 15 sec
              Aging Time 300 sec
Interface    Role          State      Cost          Priority.Number  Type
-----
##### MST2: Vlan: 2
Root ID      Priority    32770 (0x8002)
              Address    e083.bce8.9601
Bridge ID    Priority    32770 (0x8002)
              Address    e083.bce8.9601
Interface    Role          State      Int-Cost       Priority.Number  Type
-----
eth-0-48     Disabled     Discarding 20000          128.48          P2p
eth-0-1      Disabled     Discarding 20000          128.1           P2p
##### MST15: Vlan: 15
Root ID      Priority    32783 (0x800f)
              Address    e083.bce8.9601
Bridge ID    Priority    32783 (0x800f)
              Address    e083.bce8.9601
Interface    Role          State      Int-Cost       Priority.Number  Type
-----
eth-0-48     Disabled     Discarding 20000          128.48          P2p
eth-0-1      Disabled     Discarding 20000          128.1           P2p
```

Related Commands

None

3.9.47 spanning-tree instance forward**Command Purpose**

Use this command to set STP state is forward for instance and keep forward.

Command Syntax

```
spanning-tree instance INSTANCE_ID forward
```

```
no spanning-tree instance INSTANCE_ID forward
```

Parameter	Parameter Description	Parameter Value
INSTANCE_ID	Specify the identifier	1-4094

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to set STP state is forward for instance and keep forward:

```
Switch# configure terminal
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config)# interface eth-0-1
Switch(config-if)# spanning-tree instance 1 forward
Switch# configure terminal
Switch(config)# interface eth-0-1
```

Related Commands

3.10 Flow Control Commands

3.10.1 flowcontrol send

Command Purpose

Use this command to enable or disable flow control send function.

Command Syntax

flowcontrol send (on | off)

Parameter	Parameter Description	Parameter Value
on	Set send flowcontrol enable	-
off	Set send flowcontrol disable	-

Command Mode

Interface Configuration

Default

Off

Usage

Use the flowcontrol Interface Configuration command to set the interface's ability to send pause frames to on or off.

Examples

This example shows how to enable flow control on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# flowcontrol send on
```

Related Commands

flowcontrol receive on

3.10.2 flowcontrol receive

Command Purpose

Use this command to enable or disable flow control receive function.

Command Syntax

flowcontrol receive (on | off)

Parameter	Parameter Description	Parameter Value
on	Set receive flowcontrol enable	-
off	Set receive flowcontrol disable	-

Command Mode

Interface Configuration

Default

Off

Usage

Use the flowcontrol interface configuration command to set the interface's ability to receive pause frames to on or off.

Examples

This example shows how to enable flow control on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# flowcontrol receive on
```

Related Commands

flowcontrol send on

3.10.3 show flowcontrol

Command Purpose

Use this command to display flow control information.

Command Syntax

show flowcontrol (IFNAME |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

Use the command to display flowcontrol ability and the pause frame information of each port.

Examples

This example shows how to display flowcontrol information:

```
Switch# show flowcontrol
```

Port	Receive FlowControl		Send FlowControl		RxPause	TxPause
	admin	oper	admin	oper		
eth-0-1	off	off	off	off	0	0
eth-0-2	off	off	off	off	0	0
eth-0-3	off	off	off	off	0	0
eth-0-4	off	off	off	off	0	0
eth-0-5	off	off	off	off	0	0
eth-0-6	off	off	off	off	0	0
eth-0-7	off	off	off	off	0	0
eth-0-8	off	off	off	off	0	0
eth-0-9	off	off	off	off	0	0
eth-0-10	off	off	off	off	0	0
eth-0-11	off	off	off	off	0	0
eth-0-12	off	off	off	off	0	0
eth-0-13	off	off	off	off	0	0
eth-0-14	off	off	off	off	0	0
eth-0-15	off	off	off	off	0	0
eth-0-16	off	off	off	off	0	0
eth-0-17	off	off	off	off	0	0
eth-0-18	off	off	off	off	0	0
eth-0-19	off	off	off	off	0	0
eth-0-20	off	off	off	off	0	0
eth-0-21	off	off	off	off	0	0
eth-0-22	off	off	off	off	0	0
eth-0-23	off	off	off	off	0	0
eth-0-24	off	off	off	off	0	0

Related Commands

None

3.11 Layer 2 Protocols Tunneling Commands

3.11.1 l2protocol enable

Command Purpose

Use this command to enable l2protocol function globally.

Command Syntax

l2protocol enable

no l2protocol enable

Command Mode

Global Configuration

Default

None

Usage

Use this command to enable l2protocol function globally.

Examples

This example shows how to enable l2protocol function globally:

```
Switch# configure terminal
Switch(config)# l2protocol enable
```

Related Commands

show l2protocol

3.11.2 l2protocol tunnel-dmac

Command Purpose

Use this command to configure l2protocol tunnel destination MAC address.

Command Syntax

l2protocol tunnel-dmac MAC

no l2protocol tunnel-dmac

Parameter	Parameter Description	Parameter Value
MAC	L2 protocol tunnel's destination MAC address	0100.0CCD.CDD0-D2 or 010F.E200.0003

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure l2 protocol tunnel dmac. System default tunnel-dmac is 0100.0ccd.cdd0.

Examples

Following is a sample that configuring 010FE2000003 as l2 protocol tunnel dmac:

```
Switch# configure terminal
Switch(config)# l2protocol tunnel-dmac 010F.E200.0003
```

Related Commands

show l2protocol

3.11.3 l2protocol mac 1

Command Purpose

Use this command to configure l2 protocol mac address globally.

Command Syntax

l2protocol mac 1 MAC mask MASK

no l2protocol mac 1

Parameter	Parameter Description	Parameter Value
MAC	L2 Protocol MAC address. 0180.C200.0000~0180.C200.003F is used by other protocol, so this range is out of L2 Protocol MAC address control.	0180.C200.0000 ~ 0180.C2FF.FFFF
MASK	L2 Protocol MAC MASK	FFFF.FF00.0000 ~ FFFF.FFFF.FFFF

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure I2 protocol mac address globally.

Examples

This example shows how to configure I2 protocol mac address:

```
Switch# configure terminal
Switch(config)# l2protocol mac 1 0180.c222.0000 mask ffff.ffff.0000
```

Related Commands

l2protocol full-mac

3.11.4 l2protocol mac <2-6>

Command Purpose

Use this command to configure I2 protocol mac address globally.

Command Syntax

l2protocol mac MAC_NUM MAC

no l2protocol mac MAC_NUM

Parameter	Parameter Description	Parameter Value
MAC_NUM	The ID of I2 protocol MAC	2-6
MAC	The MAC address of I2 protocol MAC	0180.C200.0000 ~ 0180.C2FF.FFFF

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure I2 protocol mac address globally. Should not overlap each other.

Examples

This example shows how to configure I2 protocol mac address:

```
Switch# configure terminal
Switch(config)# l2protocol mac 3 0180.c200.0000
```

Related Commands

l2protocol full-mac

3.11.5 l2protocol

Command Purpose

Use this command to configure l2protocol pdu-mac-address to discard, peer or tunnel.

Command Syntax

l2protocol (stp | slow-proto | dot1x | cfm | mac MAC_NUM | full-mac) (discard | peer | tunnel (evc WORD |) | forward)

l2protocol (cdp | vtp | lldp | all) (discard | peer | forward)

no l2protocol (stp | slow-proto | dot1x | cfm | lldp | cdp | vtp | all | mac MAC_NUM | full-mac)

Parameter	Parameter Description	Parameter Value
stp	MAC: 0180.c200.0000	-
slow-proto	MAC: 0180.c200.0002, ethertype: 0x8809	-
dot1x	MAC: 0180.c200.0003, ethertype: 0x888e	-

Parameter	Parameter Description	Parameter Value
cfm	ethertype: 0x8902	-
cdp	Cisco Discovery Protocol	-
vtp	Vlan Trunking Protocol	-
lldp	Link Layer Discovery Protocol	-
all	include stp, sflow-proto, dot1x, cfm, lldp, cdp, vtp	-
mac MAC_NUM	Globally configured mac 1-2	1-2
discard	Discard the protocol data unit	-
peer	Act as peer to the customer device instance of the protocol, peer is default option	-
tunnel	Tunnel the protocol data unit into the SVLAN	-
forward	Forward the protocol data unit	-
full-mac	Globally configured full-mac	-
WORD	The evc name	Up to 15 characters

Command Mode

Interface Configuration

Default

None

Usage

Use this command to configure I2 protocol to discard, peer or tunnel.

Examples

This example shows how to configure I2 protocol to discard:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2protocol stp discard
```

This example shows how to configure I2 protocol to tunnel:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2protocol slow-proto tunnel evc evc1
```

Related Commands

None

3.11.6 I2protocol uplink enable

Command Purpose

Use this command to configure I2 protocol uplink port.

Command Syntax

```
I2protocol uplink enable
no I2protocol uplink enable
```

Command Mode

Interface Configuration

Default

None

Usage

Use this command to configure I2 protocol uplink port.

Examples

This example shows how to configure I2 protocol uplink port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# I2protocol uplink enable
```

Related Commands

None

3.11.7 show I2protocol

Command Purpose

Use this display current I2 protocol tunnel configuration.

Command Syntax

show I2protocol (interface IFNAME | tunnel-dmac |)

Parameter	Parameter Description	Parameter Value
interface IFNAME	Interface name	Support aggregation and physical ports
tunnel-dmac	Layer2 protocols tunnel destination MAC address	-

Command Mode

Privileged EXEC

Default

None

Usage

Use this display current I2 protocol tunnel configuration or on specified interface.

Examples

This example shows how to display current I2 protocol tunnel configuration on interface eth-0-1:

```
Switch# show I2protocol interface eth-0-1
```

Interface	PDU Address	MASK	Status	EVC
eth-0-1	stp	ffff.ffff.ffff	Peer	N/A
eth-0-1	slow-proto	ffff.ffff.ffff	Peer	N/A
eth-0-1	dot1x	ffff.ffff.ffff	Peer	N/A

```
Switch # show I2protocol tunnel-dmac
```

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd0
```

This example shows how to display current I2 protocol tunnel configuration on tunnel-mac:

```
Switch# show I2protocol tunnel-dmac
```

```
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd0
```

Related Commands

None

3.11.8 I2protocol cos

Command Purpose

Use this command to configure l2protocol cos globally.

Command Syntax

l2protocol cos COS_VALUE

no l2protocol cos

Parameter	Parameter Description	Parameter Value
COS_VALUE	vlan tag priority	0-7

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure l2protocol cos globally, the default value is 0.

Examples

This example shows how to configure l2protocol cos 7:

```
Switch# configure terminal
Switch(config)# l2protocol cos 7
```

Related Commands

None

3.11.9 l2protocol full-mac

Command Purpose

Use this command to configure l2 protocol mac address globally.

Command Syntax

l2protocol full-mac MAC

no l2protocol full-mac

Parameter	Parameter Description	Parameter Value
MAC	Destination MAC address, including all MAC addresses	0000.0000.0000 ~ FFFF.FFFF.FFFF

Command Mode

Global Configuration

Default

None

Usage

If the L2 protocol full-mac address coincides with BPDU, Slow proto, EAPOL or MAC<1-4>, the tunnel operation priority is orderly: BPDU, Slow proto, EAPOL, full-mac, mac<1-4>.

If the L2 protocol full-mac address coincides with L2 Protocol tunnel destination MAC address, the crossed L2 protocol mac address won't take effect when tunnel L2 Protocol

Examples

This example shows how to configure l2 protocol full-mac address:

```
Switch# configure terminal
Switch(config)# l2protocol full-mac 0100.0CCC.CCCC
```

Related Commands

l2protocol mac

3.12 Storm Control Commands

3.12.1 port storm-control

Command Purpose

Use the storm-control interface configuration command to enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface. Use the no form of this command to return to the default setting.

Command Syntax

storm-control (broadcast | multicast | unicast) (level LEVEL | pps PPS)

no storm-control (broadcast | multicast | unicast)

Parameter	Parameter Description	Parameter Value
broadcast	Enable broadcast storm control on the interface	-
multicast	Enable multicast storm control on the interface	-
unicast	Enable unicast storm control on the interface	-
level LEVEL	Specify the rising and falling suppression levels as a percentage of total bandwidth of the port.	0.00-100.00
pps PPS	Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.	0-1000000000

Command Mode

Interface Configuration

Default

Disabled

Usage

This command can only be configured on switchport.

Examples

This example shows how to configure storm-control broadcast on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# storm-control broadcast level 30
```

This example shows how to disable storm-control broadcast on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no storm-control broadcast
```

Related Commands

show storm-control

3.12.2 vlan storm-control

Command Purpose

Use the storm-control vlan configuration command to enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface. Use the no form of this command to return to the default setting.

Command Syntax

storm-control (broadcast | multicast | unicast) (bandwidth <1-100000000> | pps <0-1000000000>)

no storm-control (broadcast | multicast | unicast)

Parameter	Parameter Description	Parameter Value
broadcast	Enable broadcast storm control on the vlan	-
multicast	Enable multicast storm control on the vlan	-
unicast	Enable unicast storm control on the vlan	-
bandwidth <1-100000000>	Specify the rising and falling suppression levels as a rate in bits per second at which traffic is received on the vlan.	1-100000000
pps <0-1000000000>	Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the vlan.	0-1000000000

Command Mode

VLAN Configuration

Default

Disabled

Usage

This command can only be configured on vlan.

Examples

This example shows how to configure storm-control broadcast on vlan:

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# storm-control broadcast bandwidth 3000
```

This example shows how to disable storm-control broadcast on vlan:

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# no storm-control broadcast
```

Related Commands

show storm-control

3.12.3 ipg storm-control enable

Command Purpose

Use the ipg storm-control enable to let storm control calculate IPG bytes. Use the no form of this command to return to the default setting.

Command Syntax

ipg storm-control enable

no ipg storm-control enable

Command Mode

Global Configuration

Default

Disabled

Usage

This command can be configured on global configure mode.

Examples

This example shows how to configure storm-control to calculate IPG bytes:

```
Switch# configure terminal
Switch(config)# ipg storm-control enable
```

This example shows how to disable storm-control to calculate IPG bytes:

```
Switch# configure terminal
Switch(config)# no ipg storm-control enable
```

Related Commands

None

3.12.4 show storm-control

Command Purpose

Use this command to show storm-control configurations.

Command Syntax

show storm-control (interface INTERFACE |)

Parameter	Parameter Description	Parameter Value
interface INTERFACE	Interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

This command displays the storm-control configurations.

Examples

This example shows storm-control configurations:

```
Switch# show storm-control
```

This example shows storm-control configurations on interface eth-0-1:

```
Switch# show storm-control interface eth-0-1
```

Related Commands

storm-control

3.12.5 show storm-control resource

Command Purpose

Use this command to show storm-control resources.

Command Syntax

show resource storm-control

Command Mode

Privileged EXEC

Default

None

Usage

This command displays the storm-control resources.

Examples

This example shows the overall resources and usage of storm control.:

```
Switch# show resource storm-control
```

Related Commands

None

3.13 Loopback Detection Commands

3.13.1 loopback-detect enable

Command Purpose

Using the loopback-detect enable command, you can enable loopback detection on an interface.

Using the no loopback-detect enable command, you can disable loopback detection on an interface. By default, loopback detection is disabled on an interface.

Command Syntax

loopback-detect enable

no loopback-detect enable

Command Mode

Interface Configuration

Default

Disable

Usage

The loopback-detect enable command enables loopback detection on an interface. This function enables the system to detect a loopback on the interface quickly and minimizes impact of the loopback on the entire network. After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals. Loopback detection occupies CPU resources; therefore, disable this function when it is not required.

Examples

This example shows how to enable loopback detect on port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1

Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback-detect enable
```

Related Commands

show loopback-detect

3.13.2 loopback-detect packet-interval

Command Purpose

Using the loopback-detect packet-interval command, you can set the interval for sending loopback detection packets on all interfaces.

Using the `no loopback-detect packet-interval` command, you can restore the default interval for sending loopback detection packets on all interfaces.

By default, the interval for sending loopback detection packets is 5s

Command Syntax

`loopback-detect packet-interval INTERVAL`

`no loopback-detect packet-interval`

Parameter	Parameter Description	Parameter Value
INTERVAL	loopback detect packet send interval	1-300, unit:second

Command Mode

Global Configuration

Default

5 seconds

Usage

The `loopback-detect packet-interval` command is used to adjust the interval for sending loopback detection packets. After loopback detection is enabled on an interface, the interface sends loopback detection packets at the interval specified by the `loopback-detect packet-interval` command. If a shorter interval is set, the system sends more loopback detection packets in a certain period. This enables the system to detect loopbacks more quickly and accurately, but more system sources are consumed.

Examples

This example shows how to set the interval for sending loopback detection packets to 10s:

```
Switch# configure terminal
Switch(config)# loopback-detect packet-interval 10
```

Related Commands

`show loopback-detect`

3.13.3 loopback-detect recovery-interval

Command Purpose

Using the `loopback-detect recovery-interval` command, you can set the interval for interface recovery from abnormal status.

Using the `no loopback-detect recovery-interval` command, you can restore the default interval.

By default, the interval for recovery interval is the packet-interval * 3

Command Syntax

`loopback-detect recovery-interval INTERVAL`

`no loopback-detect recovery-interval`

Parameter	Parameter Description	Parameter Value
INTERVAL	recovery interval in seconds	1-255, unit:second

Command Mode

Interface Configuration

Default

Recovery-interval is packet-interval * 3

Usage

If the interface is shutdown, this command is useless.

Examples

This example shows how to set the interval for recovering to 10s:

```
Switch# configure terminal
Switch(config)# loopback-detect recovery-interval 10
```

Related Commands

show loopback-detect

3.13.4 loopback-detect delay-interval

Command Purpose

Using the loopback-detect delay interval on interface for set action.

Using the no loopback-detect delay-interval to set not delay.

Command Syntax

loopback-detect delay-interval INTERVAL

no loopback-detect delay-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	delay interval	1-255, unit:second

Command Mode

Interface Configuration

Default

None

Usage

The no loopback-detect delay-interval command is used to set on the interface, if received loopback-detect packet, then set action that set on the interface.

Examples

This example shows how to set the interval for delay set action to 5s:

```
Switch# configure terminal
Switch(config)# loopback-detect delay-interval 5
```

Related Commands

show loopback-detect

3.13.5 loopback-detect action

Command Purpose

Using the loopback-detect action command, you can configure an action to perform when a loopback is detected on an interface.

Using the no loopback-detect action command, you can restore the default action.

By default, an interface is blocked when a loopback is detected on the interface.

Command Syntax

loopback-detect action { shutdown | trap | block }

no loopback-detect action

Shutdown

Parameter	Parameter Description	Parameter Value
shutdown	Shuts down an interface when a loopback is detected on the interface.	-
Trap	Only sends a trap message when a loopback is detected.	-

Parameter	Parameter Description	Parameter Value
block	Block the interface and continue to send loopback-detect packets	-

Command Mode

Interface Configuration

Default

Trap

Usage

After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals. When a loopback is detected on the interface, the system performs an action to minimize the impact on the entire network. The loopback-detect action command configures the action.

Examples

This example shows how to configure the system action to shutdown interface eth-0-1 when a loopback occurs:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)# loopback-detect action shutdown
```

Related Commands

show loopback-detect

loopback-detect enable

3.13.6 loopback-detect packet vlan**Command Purpose**

Using the loopback-detect packet vlan command, you can specify the VLAN IDs of loopback detection packets on an interface.

Using the no loopback-detect packet vlan command, you can cancel the configuration.

By default, detection packets do not have a VLAN ID.

Command Syntax

loopback-detect packet vlan VID

no loopback-detect packet vlan VID

Parameter	Parameter Description	Parameter Value
VID	VLAN ID	1-4094

Command Mode

Interface Configuration

Default

No vlan id.

Usage

By default, loopback detection packets do not contain VLAN IDs. After the loopback-detect packet vlan command is executed on an interface, the interface sends an untagged loopback detection packet and the loopback detection packets with the specified VLAN tags. The specified VLANs exist and the interface has been added to the VLANs in tagged mode. If you run the loopback-detect packet vlan command multiple times in the same interface view, multiple VLAN IDs are specified.

You can specify a maximum of eight VLAN IDs

Examples

This example shows how to set the VLAN ID of loopback detection packets sent by interface eth-0-1 to 30:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)# loopback-detect packet vlan 30
```

Related Commands

show running-config

3.13.7 show loopback-detect

Command Purpose

Using the show loopback-detect command, you can view the loopback detection configuration and status of loopback detection enabled interfaces.

Command Syntax

show loopback-detect { interface IFNAME | packet-interval }

Parameter	Parameter Description	Parameter Value
interface IFNAME	Show loopback detection status and configuration on interface.	Support physical ports
packet-interval	Show loopback detect packet interval.	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to check the loopback detection configuration and status of each interface on which loopback detection is enabled.

Examples

Display the loopback detection configuration and status of loopback detection enabled interfaces:

```
Switch# show loopback-detect
```

```
Loopback detection packet interval(second) 5
```

Interface	Action	Status	Delay(s)	DLeft(s)	Recovery(s)	RLeft(s)	Send	Recv	Count
eth-0-47	trap	NORMAL	30	-	15	-	N/A	N/A	0
eth-0-48	trap	NORMAL	-	-	15	-	2001-01-05 034721	N/A	0

Related Commands

loopback-detect action

loopback-detect enable

3.14 MLAG Commands

3.14.1 mlag configuration

Command Purpose

The mlag configuration command enters MLAG configuration mode to configure Multichassis Link Aggregation (MLAG) features.

The no mlag configuration command removes all MLAG configuration command from running-config.

Command Syntax

mlag configuration

no mlag configuration

Command Mode

Global Configuration

Default

None

Usage

The mlag configuration command enters MLAG configuration mode to configure Multichassis Link Aggregation (MLAG) features. The exit command does not affect the configuration. The no mlag configuration command removes all MLAG configuration command from running-config.

Examples

This example shows how to enter MLAG configuration mode:

```
Switch# configure terminal
Switch(config)# mlag configuration
```

Related Commands

show mlag

3.14.2 peer-address

Command Purpose

The peer-address command specifies the peer IPv4 address for a MLAG domain.

The no peer-address command removes the MLAG peer's IPv4 address assignment by deleting the peer-address command from running-config.

Command Syntax

peer-address IP_ADDR

no peer-address

Parameter	Parameter Description	Parameter Value
IP_ADDR	MLAG peer IPv4 address	IPv4 Address

Command Mode

MLAG Configuration

Default

None

Usage

The peer-address command specifies the peer IPv4 address for a MLAG domain. MLAG control traffic is sent to the peer IPv4 address.

The no peer-address command removes the MLAG peer's IPv4 address assignment by deleting the peer-address command from running-config.

Examples

This example shows how to specify the peer IPv4 address for a MLAG domain:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# peer-address 12112
Switch(config-mlag)#
```

Related Commands

show mlag peer

3.14.3 peer-link

Command Purpose

The peer-link command specifies the interface that connects MLAG peers.

The no peer-link command removes the peer link by deleting the peer-link command from running-config

Command Syntax

peer-link IFNAME

no peer-link

Parameter	Parameter Description	Parameter Value
IFNAME	Interface for peer link.	Only support phy port or agg port

Command Mode

MLAG Configuration

Default

None

Usage

The peer-link command specifies the interface that connects MLAG peers. To form an MLAG, two switches are connected through an interface called a peer link. The peer link carries control and data traffic between the two switches.

The no peer-link command removes the peer link by deleting the peer-link command from running-config.

Examples

This example shows how to specify the interface that connects MLAG peers:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# peer-link eth-0-9
Switch(config-mlag)#
```

Related Commands

show mlag

3.14.4 timers mlag

Command Purpose

The timers mlag command specifies the keepalive interval and holdtime timers.

The no timers mlag command removes the specified timer and returns it to default value.

Command Syntax

timers mlag keepalive holdtime

no timers mlag

Parameter	Parameter Description	Parameter Value
keepalive	keepalive time interval	1-65535, unit:second
holdtime	holdtime time interval	4-65535, unit:second

Command Mode

MLAG Configuration

Default

Default keepalive interval is 60 seconds and default holdtime is 240 seconds.

Usage

The timers mlag command specifies the keepalive interval and holdtime timers. It will be take effective by next time when the peer goes to established. Between the locally configured keepalive timer and the calculated value by the remote holdtime/4 carried in open message, system uses the smaller one in actual calculation.

The no timers mlag command removes the specified timer and returns it to default value.

Examples

This example shows how to specify the keeepalive interval and holdtime timers:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# timers mlag 10 100
Switch(config-mlag)#
```

Related Commands

show mlag peer

3.14.5 reload-delay

Command Purpose

The reload-delay command specifies the period that non-peer links are disabled after an MLAG peer reboots.

The no reload-delay command restores the default value of 300 by deleting the reload-delay mlag statement from running-config.

Command Syntax

reload-delay (auto | period)

no reload-delay

Parameter	Parameter Description	Parameter Value
period	Disable link interval. The number 0 means that interface not enter into errdisable	0-86400, unit:second
auto	Auto recovery from errdisable after MLAG peer build successful.	-

Command Mode

MLAG Configuration

Default

300 seconds.

Usage

When an MLAG peer reboots, all ports except those in peer-link port-channel remain in errdisabled state for a specified period. This period allows all topology states to stabilize before the switch begins forwarding traffic. The specified period is configured by this command.

Examples

This example shows how to specify the dealy interval:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# reload-delay 100
Switch(config-mlag)#
```

Related Commands

show mlag

3.14.6 sync-orphan

Command Purpose

The sync-orphan command specifies the mlag peers to sync MAC entries on orphan port.

The no sync-orphan command disable the function.

Command Syntax

sync-orphan

no sync-orphan

Command Mode

MLAG Configuration

Default

Enable

Usage

If this function is disabled, MLAG peers will only sync those MAC entries in MLAG group.

Examples

This example shows how to specify the mlag peers to sync MAC entries on orphan port:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# sync-orphan
Switch(config-mlag)#
```

Related Commands

show mlag

3.14.7 sync-overlay**Command Purpose**

The sync-overlay command specifies the mlag peers to sync MAC entries on overlay logic port.

The no sync-overlay command disable the function.

Command Syntax

sync-overlay

no sync-overlay

Command Mode

MLAG Configuration

Default

Enable

Usage

If this function is disabled, MLAG peers will only sync those MAC entries in MLAG group.

Examples

This example shows how to specify the mlag peers to sync MAC entries on overlay logic ports:

```
Switch# configure terminal
Switch(config)# mlag configuration
Switch(config-mlag)# sync-overlay
Switch(config-mlag)#
```

Related Commands

show mlag

3.14.8 mlag

Command Purpose

The mlag command assigns an MLAG ID to a port-channel.

The no mlag command removes the MLAG ID assignment from the configuration mode interface by deleting the corresponding mlag command from running-config.

Command Syntax

mlag MLAGID

no mlag

Parameter	Parameter Description	Parameter Value
MLAGID	Number used as MLAG ID.	1-63

Command Mode

Interface Configuration

Default

None

Usage

The mlag command assigns an MLAG ID to a port-channel. MLAG peer switches form an MLAG when each switch configures the same MLAG ID to a port-channel interface. Only one MLAG ID can be assigned to an interface. An individual MLAG number cannot be assigned to more than one interface.

The no mlag command removes the MLAG ID assignment from the configuration mode interface by deleting the corresponding mlag command from running-config.

Examples

This example shows how to assigns an MLAG ID to a port-channel:

```
Switch# configure terminal
Switch(config)# interface agg1
Switch(config-if)# mlag 1
```

Related Commands

show mlag interface

3.14.9 clear mlag count

Command Purpose

The clear mlag count command clears mlag count information.

Command Syntax

clear mlag count

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to clear mlag count information which can be displayed by show mlag peer command.

Examples

This example shows how to clear mlag count information and display information about the MLAG peer:

```
Switch# clear mlag count
Switch# show mlag peer
```

```
MLAG neighbor is 12112, MLAG version 1
MLAG state = Established, up for 000039
Last read 000015, hold time is 240, keepalive interval is 60 seconds
Received 0 messages,Sent 0 messages
Open      received 0, sent 0
KAlive    received 0, sent 0
Fdb sync  received 0, sent 0
Failover  received 0, sent 0
Conf      received 0, sent 0
Syspri    received 0, sent 0
Peer fdb  received 0, sent 0
STP Total received 0, sent 0
  Global  received 0, sent 0
  Packet  received 0, sent 0
  Instance received 0, sent 0
  State   received 0, sent 0
Connections established 1; dropped 0
Local host 12111, Local port 61000
Foreign host 12112, Foreign port 37335
remote_sysid 0ecb30301100
```

Related Commands

```
show mlag peer
```

3.14.10 show mlag

Command Purpose

The show mlag command displays information about the MLAG configuration.

Command Syntax

```
show mlag
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display information about the MLAG configuration.

Examples

This example shows how to display information about the MLAG configuration:

```
Switch# show mlag
```

```
MLAG configuration
```

```
-----
role          Master
local_sysid   001e080a6fca
remote_sysid  0000000000000
mlag_sysid    001e080a6fca
local_syspri  32768
```

```
remote_syspri 0
mlag_syspri 32768
peer-link -
peer conf No
reload-delay 300
```

Related Commands

mlag configuration

3.14.11 show mlag peer

Command Purpose

The show mlag peer command displays information about the MLAG peer.

Command Syntax

show mlag peer (vlan-if |)

Parameter	Parameter Description	Parameter Value
vlan-if	Vlan interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display information about the MLAG peer.

Examples

This example shows how to display information about the MLAG peer:

```
Switch# show mlag peer
```

```
MLAG neighbor is 12112, MLAG version 1
MLAG state = Established, up for 4d02h14m
Last read 000029, hold time is 240, keepalive interval is 60 seconds
Received 6835 messages,Sent 7185 messages
Open      received 1, sent 2
KAlive    received 6831, sent 6830
Fdb sync  received 0, sent 0
Failover  received 0, sent 87
Conf      received 1, sent 1
STP Total received 2, sent 265
  Global  received 2, sent 3
  Packet  received 0, sent 0
  Instance received 0, sent 0
  State   received 0, sent 262
Connections established 1; dropped 0
Local host 12111, Local port 61000
Foreign host 12112, Foreign port 34283
remote_sysid 5e266a03d400
```

Related Commands

peer-address

3.14.12 show mlag interface

Command Purpose

The show mlag interface command displays information about the MLAG interface.

Command Syntax

show mlag interface (MLAGID |)

Parameter	Parameter Description	Parameter Value
MLAGID	Number used as MLAG ID.	1-63

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display information about the MLAG interface.

Examples

This example shows how to display information about the MLAG interface:

```
Switch# show mlag interface
```

mlagid	local-if	local-state	remote-state
1	agg1	up	up
2	agg2	up	up

Related Commands

mlag MLAGID

3.15 Hash Load-balance Commands

3.15.1 hash field

Command Purpose

Use this command to set hash field or create a new hash field, and enter hash field configure view;use the no command to delete user-defined hash field.

Command Syntax

hash-field (port-channel | ecmp | NAME)

no hash-field NAME

Parameter	Parameter Description	Parameter Value
port-channel	Port-channel of system default hash field	-
ecmp	Ecmp of system default hash field	-
NAME	Hash field name string	The initial character of name should be a-z, A-Z, or 0-9, character only can be 0-9A-Za-z- _ and the max length is 64

Command Mode

Global Configuration

Default

port-channel, ecmp

Usage

The system support the max number of hash field is 4, including 2 system default hash fields named port-channel and ecmp and 2 user-defined hash fields.when applied to the hash value,it can't be deleted.

Examples

The following example shows how to create a new hash field named user:

```
Switch# configure terminal
Switch(config)# hash-field user
Switch(config-hash-field)#
```

The following example shows how to delete the user-defined hash field named user:

```
Switch# configure terminal
Switch(config)# no hash-field user
```

Related Commands

show hash-field

3.15.2 I2

Command Purpose

Use this command to set I2 packet hash field; use the no command to set the I2 packet field to default.

Command Syntax

I2 (macda | macsa | vlan | eth-type | src-interface)

no I2

Parameter	Parameter Description	Parameter Value
macda	MAC Destination Address	-
macsa	MAC Source Address	-
vlan	Vlan	-
eth-type	Ethernet Type	-
src-interface	Source Interface	-

Command Mode

Config-hash-field

Default

I2 macsa macda

Usage

None

Examples

The following example shows how to select macsa for I2 packet load balance in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# I2 macsa
```

The following example shows how to select default I2 packet load balance in port-channel:


```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no l2
```

Related Commands

show hash-field

3.15.3 ip**Command Purpose**

Use this command to set ip packet hash field; use the no command to set the ip packet field to default.

Command Syntax

ip (ipda | ipsa | ip-protocol | sourceport | destport | src-interface)

no ip

Parameter	Parameter Description	Parameter Value
ipda	IP Destination Address	-
ipsa	IP Source Address	-
ip-protocol	IP Header protocol	-
sourceport	Layer4 Source Port	-
destport	Layer4 Destination Port	-
src-interface	Source Interface	-

Command Mode

Config-hash-field

Default

ip ipsa ipda sourceport destport ip-protocol

Usage

None

Examples

The following example shows how to select ipsa for ip packet load balance in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# ip ipsa
```

The following example shows how to select default ip packet load balance in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no ip
```

Related Commands

show hash-field

3.15.4 ipv6**Command Purpose**

Use this command to set ipv6 packet hash field; use the no command to set the ipv6 field to default.

Command Syntax

ipv6 (ipda | ipsa | ip-protocol | sourceport | destport | src-interface)

no ipv6

Parameter	Parameter Description	Parameter Value
ipda	IP Destination Address	-
ipsa	IP Source Address	-
ip-protocol	IP Header protocol	-
sourceport	Layer4 Source Port	-
destport	Layer4 Destination Port	-
src-interface	Source Interface	-

Command Mode

Config-hash-field

Default

ipv6 ipsa ipda sourceport destport ip-protocol

Usage

Only when the system is in ipv6 mode, the ipv6 packet hash field can work normally.

Examples

The following example shows how to select ipsa for ipv6 packet load balance in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# ipv6 ipsa
```

The following example shows how to select default ipv6 packet load balance in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no ipv6
```

Related Commands

show hash-field

3.15.5 disable control

Command Purpose

Use this command to force ip packet ,ipv6 packet or mpls packet to follow I2 hash configuration.

To return the configuration to default value use the no form of this command.

Command Syntax

```
ip disable
no ip disable
ipv6 disable
no ipv6 disable
mpls disable
no mpls disable
```

Command Mode

Config-hash-field

Default

no ip disable

no ipv6 disable

no mpls disable

Usage

None

Examples

The following example shows how to not select ipv6 packet field to hash in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# ipv6 disable
```

The following example shows how to select ipv6 packet field to hash in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no ipv6 disable
```

Related Commands

show hash-field

3.15.6 ipv6 address compress

Command Purpose

Use this command to change ipv6 packet's IP address compressing mode.

To return the configuration to default value use the no form of this command.

Command Syntax

ipv6 address compress mode (xor | lsb)

no ipv6 address compress mode

Parameter	Parameter Description	Parameter Value
xor	Xor Compressing Mode	-
lsb	Lsb Compressing Mode	-

Command Mode

Config-hash-field

Default

ipv6 address compress mode xor

Usage

None

Examples

The following example shows how to set ipv6 address compressing mode to lsb:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# ipv6 address compress mode lsb
```

The following example shows how to set ipv6 address compressing mode to default:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no ipv6 address compress mode
```

Related Commands

show hash-field

3.15.7 hash seed

Command Purpose

Use this command to set hash seed.

To return the configuration to default value use the no form of this command.

Command Syntax

seed (<0-4294967295> | router-id | random)

no seed

Parameter	Parameter Description	Parameter Value
<0-4294967295>	User Define	-
router-id	Use Router-id As Hash Seed	-
random	Random Value	-

Command Mode

Config-hash-field

Default

seed 0

Usage

None

Examples

The following example shows how to use router-id as hash seed:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# seed router-id
```

The following example shows how to set hash seed to default:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no seed
```

Related Commands

show hash-field

3.15.8 hash arithmetic

Command Purpose

Use this command to set hash arithmetic.

To return the configuration to default value use the no form of this command.

Command Syntax

hash-arithmetic first (xor8 | xor16 | crc8-1 | crc8-2 | crc10-1 | crc10-2 | crc16-1 | crc16-2 | crc16-3 | crc16-4) second (xor8 | xor16 | crc8-1 | crc8-2 | crc10-1 | crc10-2 | crc16-1 | crc16-2 | crc16-3 | crc16-4)

no hash-arithmetic

Parameter	Parameter Description	Parameter Value
crc	Cyclical redundancy check arithmetic	-

Parameter	Parameter Description	Parameter Value
xor	Exclusive or arithmetic	-

Command Mode

Config-hash-field

Default

hash-arithmetic first xor16 second crc16-1

Usage

None

Examples

The following example shows how to set first hash arithmetic and second hash arithmetic in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# hash-arithmetic first xor16 second xor8
```

The following example shows how set default first hash arithmetic and second hash arithmetic in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no hash-arithmetic
```

Related Commands

show hash-field

3.15.9 hash symmetry**Command Purpose**

Use this command to enable hash symmetry function.

To return the configuration to default value use the no form of this command.

Command Syntax

mode symmetry
no mode symmetry

Command Mode

Config-hash-field

Default

no mode symmetry

Usage

None

Examples

The following example shows how to set hash symmetry in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# mode symmetry
```

The following example shows how to set hash symmetry to default in port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# no mode symmetry
```

Related Commands

show hash-field

3.15.10 description**Command Purpose**

Use this command to configure the description for hash field; use the no command to delete the description.

Command Syntax

description LINE

no description

Parameter	Parameter Description	Parameter Value
LINE	Hash field description	The description should be no more than 128 characters

Command Mode

Config-hash-field

Default

None

Usage

None

Examples

The following example shows how to set description for port-channel:

```
Switch# configure terminal
Switch(config)# hash-field port-channel
Switch(config-hash-field)# description this is port-channel
```

The following example shows how to delete description for port-channel:

Related Commands

show hash-field

3.15.11 show hash-field**Command Purpose**

Use this command to display the configurations and statistics on all hash fields or a hash field.

Command Syntax

show hash-field (port-channel | ecmp | NAME |)

Parameter	Parameter Description	Parameter Value
port-channel	Port-channel of system default hash field	-
ecmp	Ecmp of system default hash field	-
NAME	Hash field name string	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the configurations and statistics on the port-channel:

```
Switch# show hash-field port-channel
```

```
hash-field name: port-channel
```

```
description: this is port-channel
```

Option	Control type
ipv6 address compress	xor
hash seed	user set (0)
hash arithmetic first	xor16
hash arithmetic second	crc16-1
hash symmetry	disable
ip	enable
ipv6	enable
mpls	enable

hash field select		
Packet	HashField	
l2:	macsa	macda
ip:	ipsa l4-sourceport ip-protocol	ipda l4-destport
ipv6:	ipsa l4-sourceport ip-protocol	ipda l4-destport
gre:	ipsa gre-key	ipda
vxlan:	vni outer-ipda	outer-l4-sourceport outer-ipsa
nvgre:	vsid outer-ipsa	outer-ipda
mpls:	top-label	2nd-label
vpws:	top-label	2nd-label
vpls(inner-l2):	inner-macda	inner-macsa
vpls(inner-l3):	inner-ipda	inner-ipsa
l3vpn:	inner-ipsa inner-ip-protocol inner-l4-destport	inner-ipda inner-l4-sourceport

Related Commands

None

3.15.12 hash value

Command Purpose

Use this command to create a hash value and enter hash value configure view; use the no command to delete the hash value.

Command Syntax

hash-value NAME

no hash-value NAME

Parameter	Parameter Description	Parameter Value
NAME	Hash value name string	The initial character of name should be a-z, A-Z, or 0-9, character only can be 0-9A-Za-z-._ and the max length is 64

Command Mode

Global Configuration

Default

None

Usage

The system support the max number of hash value is 63.when applied to the interface,it can't be deleted.

Examples

The following example shows how to create hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)#
```

The following example shows how to delete hash value aaa:

```
Switch# configure terminal
Switch(config)# no hash-value aaa
```

Related Commands

show hash-value

3.15.13 port-channel select

Command Purpose

Use this command to select hash field and hash arithmetic for all mode linkagg; use the no command to delete the configuration.

Command Syntax

port-channel select NAME hash-arithmetic (first | second)

no port-channel select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

If there is only "port-channel select" configuration in the hash value, the hash value can apply on the agg output and input.

If the hash value has "port-channel static select" configuration or "port-channel dynamic select" configuration, the hash value only can be applied on input port.

Examples

The following example shows how to select hash field and hash arithmetic for linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no port-channel select
```

Related Commands

show hash-value

3.15.14 port-channel static select

Command Purpose

Use this command to select hash field and hash arithmetic for static linkagg; use the no command to delete the configuration.

Command Syntax

port-channel static select NAME hash-arithmetic (first | second)

no port-channel static select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "port-channel select NAME hash-arithmetic (first | second)" for static mode linkagg.

Examples

The following example shows how to select hash field and hash arithmetic for static mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel static select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for static mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no port-channel static select
```

Related Commands

show hash-value

3.15.15 port-channel dynamic select

Command Purpose

Use this command to select hash field and hash arithmetic for dynamic linkagg; use the no command to delete the configuration.

Command Syntax

port-channel dynamic select NAME hash-arithmetic (first | second)

no port-channel dynamic select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "port-channel dynamic select NAME hash-arithmetic (first | second)" for dynamic mode linkagg.

Examples

The following example shows how to select hash field and hash arithmetic for dynamic mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel dynamic select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for dynamic mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no port-channel dynamic select
```

Related Commands

show hash-value

3.15.16 port-channel resilient select

Command Purpose

Use this command to select hash field and hash arithmetic for resilient linkagg; use the no command to delete the configuration.

Command Syntax

port-channel resilient select NAME hash-arithmetic (first | second)

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "port-channel select NAME hash-arithmetic (first | second)" for resilient mode linkagg.

Examples

The following example shows how to select hash field and hash arithmetic for resilient mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# port-channel resilient select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for static mode linkagg in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no port-channel resilient select
```

Related Commands

show hash-value

3.15.17 ecmp select**Command Purpose**

Use this command to select hash field and hash arithmetic for all mode ecmp; use the no command to delete the configuration.

Command Syntax

ecmp select NAME hash-arithmetic (first | second)

no ecmp select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command can configure the static, dynamic or dynamic flow id mode.

If ecmp has static, dynamic or dynamic flow id set on the command mode, this command has low priority level.

Examples

The following example shows how to select hash field and hash arithmetic for all mode ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# ecmp select user hash-arithmetic first
```

The following example shows how to delete the ecmp select configuration in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no ecmp select
```

Related Commands

show hash-value

3.15.18 ecmp dynamic select**Command Purpose**

Use this command to select hash field and hash arithmetic for dynamic mode ecmp; use the no command to delete the configuration.

Command Syntax

ecmp dynamic select NAME hash-arithmetic (first | second)

no ecmp dynamic select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for dynamic mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for dynamic ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# ecmp dynamic select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for dynamic ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no ecmp dynamic select
```

Related Commands

show hash-value

3.15.19 ecmp dynamic flow-id select**Command Purpose**

Use this command to select hash field and hash arithmetic for dynamic flow mode; use the no command to delete the configuration.

Command Syntax

ecmp dynamic flow-id select NAME hash-arithmetic (first | second)

no ecmp dynamic flow-id select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for dynamic flow-id mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for dynamic flow id ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# ecmp dynamic flow-id select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for dynamic flow id ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no ecmp dynamic flow-id select
```

Related Commands

show hash-value

3.15.20 ecmp static select

Command Purpose

Use this command to select hash field and hash arithmetic for static mode ecmp; use the no command to delete the configuration.

Command Syntax

ecmp static select NAME hash-arithmetic (first | second)

no ecmp static select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for static mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for static ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# ecmp static select user hash-arithmetic first
```

The following example shows how to delete hash field and hash arithmetic for static ecmp in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no ecmp static select
```

Related Commands

show hash-value

3.15.21 ecmp static select packet

Command Purpose

Use this command to select hash field and hash arithmetic for static mode ecmp of L3/nvgre/vxlan packet; use the no command to delete the configuration.

Command Syntax

ecmp static select NAME hash-arithmetic (first | second) l3

no ecmp static select l3

ecmp static select NAME hash-arithmetic (first | second) nvgre

no ecmp static select nvgre

ecmp static select NAME hash-arithmetic (first | second) vxlan

no ecmp static select vxlan

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value

Default

None

Usage

This command has a higher priority than command "ecmp static select NAME hash-arithmetic (first | second)" for static mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for static ecmp of L3 packet in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# ecmp static select user hash-arithmetic first l3
```

ecmp of L3 packet The following example shows how to delete hash field and hash arithmetic for static in hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no ecmp static select l3
```

Related Commands

show hash-value

3.15.22 description

Command Purpose

Use this command to configure the description for hash value; use the no command to delete the description.

Command Syntax

description LINE

no description

Parameter	Parameter Description	Parameter Value
LINE	Hash value description	The description should be no more than 128 characters

Command Mode

Config-hash-value

Default

None

Usage

None

Examples

The following example shows how set description for hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# description this is hash-value aaa
```

The following example shows how delete description for hash value aaa:

```
Switch# configure terminal
Switch(config)# hash-value aaa
Switch(config-hash-value)# no description
```

Related Commands

show hash-value

3.15.23 show hash-value**Command Purpose**

Use this command to display the configurations of a hash value or all hash value.

Command Syntax

show hash-value (NAME |)

Parameter	Parameter Description	Parameter Value
NAME	Hash value name string	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the configurations of hash value:

```
Switch# show hash-value

LBT:load balance type      LBM:load balance mode
PT :packet type            HF :hash field
HA :hash arithmetic
hash-value name: aaa
LBT      LBM      PT      HF      HA
```

port-channel	static	all	NOCFG	NOCFG
port-channel	dynamic	all	NOCFG	NOCFG
port-channel	resilient	all	NOCFG	NOCFG
ecmp	static	l3	NOCFG	NOCFG
ecmp	static	nvgre	NOCFG	NOCFG
ecmp	static	vxlان	NOCFG	NOCFG
ecmp	dynamic	all	NOCFG	NOCFG
ecmp	flow id	all	NOCFG	NOCFG

Related Commands

None

3.15.24 show hash-value interface-applied

Command Purpose

Use this command to display the relationship between hash value and interface.

Command Syntax

show hash-value interface-applied

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the relationship between hash value paorfile and interface:

```
Switch# show hash-value interface-applied
```

```
eth-0-1
  hash-value aaa input
```

Related Commands

None

3.15.25 hash value applied to interface

Command Purpose

Use this command to apply a hash value to interface; use the no command to remove the hash-value from interface.

Command Syntax

load-balance hash-value NAME (input | output)

no load-balance hash-value (input | output)

Parameter	Parameter Description	Parameter Value
NAME	Hash value name	-
input	Input direction	-
output	Output direction	-

Command Mode

Interface Configuration

Default

None

Usage

Physical port only can select input direction, linkagg port can select input direction and output direction. Agg member port can't configure the command.

Examples

The following example shows how to apply a hash value to eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# load-balance hash-value aaa input
```

The following example shows how to remove a hash value from eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no load-balance hash-value input
```

Related Commands

show hash-value interface-applied

3.15.26 hash value applied to acl**Command Purpose**

Use this command to make a hash value be acl action.

To remove the configuration, use the no form of this command.

Command Syntax

load-balance hash-value NAME

no load-balance hash-value

Parameter	Parameter Description	Parameter Value
NAME	Hash value name	-

Command Mode

Config-pmap-c

Default

None

Usage

Acl action has highest priority.

Examples

The following example shows how to make a hash value be acl action:

```
Switch# configure terminal
Switch(config)# policy-map pmap1
Switch(config-pmap)# class cmap1
Switch(config-pmap-c)# load-balance hash-value aaa
```

The following example shows how to remove a hash value from acl action:

```
Switch# configure terminal
Switch(config)# policy-map pmap1
Switch(config-pmap)# class cmap1
Switch(config-pmap-c)# no load-balance hash-value
```

Related Commands

None

3.15.27 hash-value global**Command Purpose**

Use this command to enter hash value global configure view.

Command Syntax

hash-value global

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to enter hash value global view:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)#
```

Related Commands

show hash-value global

3.15.28 port-channel select**Command Purpose**

Use this command to select hash field and hash arithmetic for linkagg; use the no command to set the default configuration.

Command Syntax

port-channel select NAME hash-arithmetic (first | second)

no port-channel select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

port-channel

Usage

Compared with hash value configuration, this command has lower priority

Examples

The following example shows how to select hash field and hash arithmetic for linkagg in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# port-channel select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for linkagg in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no port-channel select
```

Related Commands

show hash-value global

3.15.29 ecmp select

Command Purpose

Use this command to select hash field and hash arithmetic for all mode ecmp; use the no command to set the default configuration.

Command Syntax

ecmp select NAME hash-arithmetic (first | second)

no ecmp select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

ecmp

Usage

This command can configure the static, dynamic or dynamic flow id mode.

If ecmp has static, dynamic or dynamic flow id set on the command mode, this command has low priority level.

Examples

The following example shows how to select hash field and hash arithmetic for all mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for all mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no ecmp select
```

Related Commands

show hash-value global

3.15.30 ecmp dynamic select

Command Purpose

Use this command to select hash field and hash arithmetic for dynamic mode ecmp; use the no command to set the default configuration.

Command Syntax

ecmp dynamic select NAME hash-arithmetic (first | second)

no ecmp dynamic select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

ecmp

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for dynamic mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for dynamic mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp dynamic select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for dynamic mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no ecmp dynamic select
```

Related Commands

show hash-value global

3.15.31 ecmp dynamic flow-id select

Command Purpose

Use this command to select hash field and hash arithmetic for dynamic flow mode ecmp; use the no command to set the default configuration.

Command Syntax

ecmp dynamic flow-id select NAME hash-arithmetic (first | second)

no ecmp dynamic flow-id select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

ecmp

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for dynamic flow id mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for dynamic flow mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp dynamic flow-id select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for dynamic flow mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no ecmp dynamic flow-id select
```

Related Commands

show hash-value global

3.15.32 ecmp static select

Command Purpose

Use this command to select hash field and hash arithmetic for static mode ecmp; use the no command to set the default configuration.

Command Syntax

ecmp static select NAME hash-arithmetic (first | second)

no ecmp static select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

ecmp

Usage

This command has a higher priority than command "ecmp select NAME hash-arithmetic (first | second)" for static mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for static mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp static select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for static mode ecmp in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no ecmp static select
```

Related Commands

show hash-value global

3.15.33 ecmp static select packet

Command Purpose

Use this command to select hash field and hash arithmetic for static mode ecmp of L3/nvgre/vxlan packet; use the no command to delete the configuration.

Command Syntax

ecmp static select NAME hash-arithmetic (first | second) l3

no ecmp static select l3

ecmp static select NAME hash-arithmetic (first | second) nvgre

no ecmp static select nvgre

ecmp static select NAME hash-arithmetic (first | second) vxlan

no ecmp static select vxlan

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

None

Usage

This command has a higher priority than command "ecmp static select NAME hash-arithmetic (first | second)" for static mode ecmp.

Examples

The following example shows how to select hash field and hash arithmetic for static ecmp of L3 packet in hash value global :

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# ecmp static select user hash-arithmetic first l3
```

The following example shows how to delete hash field and hash arithmetic for static ecmp of L3 packet in hash value global:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no ecmp static select l3
```

Related Commands

show hash-value global

3.15.34 efd hash

Command Purpose

Use this command to set the fields of the efd hash.

To return the configuration to default value,use the no form of this command.

Command Syntax

efd select { ipda | ipsa | macda | macsa | sourceport | destport | ip-protocol | vxlan-vni | nvgre-vsids | inner-ipda | inner-ipsa | inner-ip-protocol | inner-macda | inner-macsa | inner-sourceport | inner-destport | src-interface }

no efd select

Parameter	Parameter Description	Parameter Value
ipda	IP Source Address	-
ipsa	IP Destination Address	-
macda	MAC Source Address	-
macsa	MAC Destination Address	-

Parameter	Parameter Description	Parameter Value
sourceport	Layer4 Source Port	-
destport	Layer4 Destination Port	-
ip-protocol	IP Header protocol	-
vxlان-vni	VXLAN VNI	-
nvgre-vsíd	NVGRE VSID	-
inner-ipda	Inner header's IP Destination Address	-
inner-ipsa	Inner header's IP Source Address	-
inner-ip-protocol	Inner header's IP Header protocol	-
inner-macda	Inner header's MAC Destination Address	-
inner-macsa	Inner header's MAC Source Address	-
inner-sourceport	Inner header's Layer4 Source Port	-
inner-destport	Inner header's Layer4 Destination Port	-
src-interface	Source Interface	-

Command Mode

Config-hash-value-global

Default

ipda ipsa macda macsa sourceport destport ip-protocol

Usage

EFD flow hash has the same value with this command configuration.

Examples

The following example shows how to set fields for EFD hash:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# efd select ipsa ipda
```

The following example shows how to delete fields for EFD hash:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no efd select
```

Related Commands

show hash-value global

3.15.35 Iuid select

Command Purpose

Use this command to select hash field and hash arithmetic for linkagg and it only works for no unicast packets; use the no command to set the default configuration.

Command Syntax

Iuid select NAME hash-arithmetic (first | second)

no Iuid select

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

port-channel

Usage

None

Examples

The following example shows how to select hash field and hash arithmetic for linkagg and it works when packet is not unicast:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# lbid select user hash-arithmetic first
```

The following example shows how to set default hash field and hash arithmetic for linkagg and it works when packet is not unicast:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no lbid select
```

Related Commands

show hash-value global

3.15.36 entropy select**Command Purpose**

Use this command to set the fields of the entropy hash.

To return the configuration to default value, use the no form of this command.

Command Syntax

entropy select NAME hash-arithmetic (first | second)

Parameter	Parameter Description	Parameter Value
NAME	Hash field name string	-
first	First hash arithmetic	-
second	Second hash arithmetic	-

Command Mode

Config-hash-value-global

Default

None

Usage

None

Examples

The following example shows how to set fields for entropy hash:


```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# entropy select usr hash-arithmetic first
```

The following example shows how to delete fields for entropy hash:

```
Switch# configure terminal
Switch(config)# hash-value global
Switch(config-hash-value-global)# no entropy select
```

Related Commands

show hash-value global

3.15.37 disable ecmp round-robin

Command Purpose

Use this command to disable ecmp round robin load balance as a acl action.

To remove the configuration,use the no form of this command.

Command Syntax

```
ecmp load-balance round-robin disable
no ecmp load-balance round-robin disable
```

Command Mode

Config-pmap-c

Default

None

Usage

None

Examples

The following example shows how to disable ecmp round-robin as a acl action:

```
Switch# configure terminal
Switch(config)# policy-map map1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# ecmp load-balance round-robin disable
```

The following example shows how to enable ecmp round-robin as a acl action:

```
Switch# configure terminal
Switch(config)# policy-map map1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# no ecmp load-balance round-robin disable
```

Related Commands

None

3.15.38 disable port-channel round-robin

Command Purpose

Use this command to disable linkagg round robin load balance as a acl action.

To remove the configuration,use the no form of this command.

Command Syntax

```
port-channel load-balance round-robin disable
```

no port-channel load-balance round-robin disable

Command Mode

Config-pmap-c

Default

None

Usage

None

Examples

The following example shows how to disable linkagg round-robin as a acl action:

```
Switch# configure terminal
Switch(config)# policy-map map1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# port-channel load-balance round-robin disable
```

The following example shows how to enable linkagg round-robin as a acl action:

```
Switch# configure terminal
Switch(config)# policy-map map1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# no port-channel load-balance round-robin disable
```

Related Commands

None

Chapter 4 IP Service Commands

4.1 ARP Commands

4.1.1 Arp

Command Purpose

To add a permanent entry in the Address Resolution Protocol (ARP) cache, use the arp command in global configuration mode.

To remove an entry from the ARP cache, use the no form of this command.

Command Syntax

```
arp ( vrf VRF-NAME | ) IP-ADDRESS HARDWARE-ADDRESS
```

```
no arp ( vrf VRF-NAME | ) IP-ADDRESS
```

Parameter	Parameter Description	Parameter Value
vrf VRF-NAME	Virtual Routing and Forwarding (VRF) instance. The vrf-name argument is the name of the VRF table	String with up to 15 characters
IP-ADDRESS	IP address in four-part dotted decimal format corresponding to the local data-link address	IPv4 Address
HARDWARE-ADDRESS	Local data-link address (a 48-bit address)	MAC Address

Command Mode

Global Configuration

Default

No entries are permanently installed in the ARP cache.

Usage

Because most hosts support dynamic resolution, you generally need not specify static ARP cache entries.

To remove all none static entries from the ARP cache, use the clear arp-cache privileged EXEC command.

Examples

The following is an example of add a static ARP entry for a typical Ethernet host:

```
Switch# configure terminal
Switch(config)# arp 10.31.7.19 0800.0900.1834
```

Related Commands

clear arp-cache

4.1.2 arp retry-interval

Command Purpose

When an interface requests a mapping for an address not in the cache, system will send ARP request message on the associated network requesting the address mapping. Usually, 3 request messages will be sent until the system got a response. To configure the ARP request delay interval between 2 messages, use arp retry-interval command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

arp retry-interval *SECONDS*

no arp retry-interval

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) that an ARP request delay to interface	0-3 seconds

Command Mode

Interface Configuration

Default

1 second

Usage

This command is ignored when issued on interfaces that do not use ARP. The show interface EXEC command displays the ARP retry interval value. The value as seen in the following example from the show interface command:

ARP timeout 01:00:00, ARP retry interval 1s

Examples

The following example sets the ARP retry interval to 3 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
Switch(config-if)# arp retry-interval 3
```

Related Commands

show interface

4.1.3 arp timeout

Command Purpose

Use this command to set the arp timeout value. Use the no form of this command to restore the default value.

Command Syntax

arp timeout *SECONDS*

no arp timeout

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) that an entry remains in the ARP cache.	1-2147483 seconds
	<1-2147483>	

Command Mode

Interface Configuration

Default

3600 seconds (1 hour)

Usage

This command is ignored when issued on interfaces that do not use ARP. The show interface EXEC command displays the ARP timeout value. The value as seen in the following example from the show interface command:

```
ARP timeout 01:00:00, ARP retry interval 1s
```

Examples

The following example sets the ARP timeout to 1200 seconds to allow entries to time out more quickly than the default:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
Switch(config-if)# arp timeout 1200
```

Related Commands

show interface

4.1.4 arp as-layer-3 enable

Command Purpose

To set that deal with the arp packet as layer3 packet. To disable arp as-layer-3, use the no form of this command.

Command Syntax

```
arp as-layer-3 enable
no arp as-layer-3 enable
```

Command Mode

Global Configuration

Default

Disable

Usage

vlan classifier and IGMP Snooping affected by the CLI.

Enable, vlan classifier activate base ip, the arp packet matched source ip address will classifier to specified vlan. Otherwise, not classifier to specified vlan.

Enable, ip source guard enable the ip check on the port, the arp packet matched source ip address will not filter. Otherwise, will filter.

Examples

The following example show how to enable arp as-layer-3:

```
Switch# configure terminal
Switch(config)# arp as-layer-3 enable
```

Related Commands

N/A

4.1.5 arp fake global enable

Command Purpose

To enable fake arp global, use the no form of this command. To disable arp fake global, use the no form of this command.

Command Syntax

arp fake global enable
no arp fake global enable

Command Mode

Global Configuration

Default

Disable

Usage

Not effect until both enable global and interface arp fake.

Examples

The following example show how to enable global fake arp:

```
Switch# configure terminal  
Switch(config)# arp fake global enable
```

Related Commands

arp fake enable

4.1.6 arp fake enable

Command Purpose

To enable fake arp on interface, use the no form of this command.

Command Syntax

arp fake enable
no arp fake enable

Command Mode

Interface Configuration

Default

Enable

Usage

If enable, the interface receive IP packets that not match any ARP entry will create an fake ARP entry. Before interface received ARP reply, the IP packets matched the fake ARP entry will be dropped. After interface received ARP reply, will create active ARP entry instead of fake ARP entry.

Examples

The following example show how to enable fake arp:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# arp fake enable
```

Related Commands

arp fake global enable

4.1.7 arp fake timeout

Command Purpose

To configure how long a fake entry remains in the ARP cache, use the arp fake timeout command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

arp fake timeout *SECONDS*
no arp fake timeout

Parameter	Parameter Description	Parameter Value
SECONDS	Time that a fake entry remains in the ARP cache.	1-36000, unit:second

Command Mode

Interface Configuration

Default

5 seconds

Usage

When switch was attached, can let the fake ARP entry to time out later.

Examples

The following example sets the ARP fake timeout to 100 seconds to allow entries to time out:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# arp fake timeout 100
```

Related Commands

N/A

4.1.8 clear arp-cache

Command Purpose

To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the clear arp-cache command in privileged EXEC mode.

Command Syntax

clear arp-cache ((vrf *VRF-NAME* |) interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
vrf VRF-NAME	(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance	String with up to 15 characters
IFNAME	(Optional) Refreshes only the ARP table entries associated with this interface	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command updates the dynamically learned IP address and MAC address mapping information in the ARP table to ensure the validity of those entries. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), those entries are aged out of the ARP table immediately as opposed to at the next refresh interval.

Use this command without any arguments or keywords to refresh all ARP cache entries for all enabled interfaces.

Examples

The following example shows how to refresh all dynamically learned ARP cache entries for all enabled interfaces:

```
Switch# clear arp-cache
```

Related Commands

show ip arp

4.1.9 clear ip arp

Command Purpose

To refresh the specific dynamically created entry from the Address Resolution Protocol (ARP) cache, use the clear ip arp command in privileged EXEC mode.

Command Syntax

```
clear ip arp ( vrf VRF-NAME | ) IP-ADDRESS
```

Parameter	Parameter Description	Parameter Value
	(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance	
vrf <i>VRF-NAME</i>		String with up to 15 characters

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	(Optional) Refreshes only the ARP table entries associated with this IP address	-

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command updates the specific dynamically learned IP address and MAC address mapping information in the ARP table. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), the entry is aged out of the ARP table immediately as opposed to at the next refresh interval.

Examples

The following example shows how to refresh the dynamically learned ARP entries 10.10.10.10:

```
Switch# clear ip arp 10.10.10.10
```

Related Commands

show ip arp

4.1.10 clear ip arp statistics

Command Purpose

To clear ARP packets statistics processed by system, use the clear ip arp statistics command in privileged EXEC mode.

Command Syntax

```
clear ip arp ( vrf VRF-NAME | ) statistics
```

Parameter	Parameter Description	Parameter Value
vrf VRF-NAME	(Optional) Clear ARP statistics for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance	String with up to 15 characters

Command Mode

Privileged EXEC

Default

No default behavior or values.

Usage

This command use to clear ARP packets statistics.

Examples

The following example shows how to clear ARP packets statistics:

```
Switch# clear ip arp statistics
```

Related Commands

show ip arp summary

4.1.11 show ip arp

Command Purpose

To display the entries in the Address Resolution Protocol (ARP) table, use the show ip arp command in privileged EXEC mode.

Command Syntax

```
show ip arp ( ( vrf VRF-NAME | ) interface INTERFACE-NAME | )
```

Parameter	Parameter Description	Parameter Value
vrf <i>VRF-NAME</i>	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the vrf-name argument	String with up to 15 characters
<i>INTERFACE-NAME</i>	(Optional) Refreshes only the ARP table entries associated with this interface	-

Command Mode

Privileged EXEC

Default

None

Usage

To display all entries in the ARP cache, use this command without any arguments or keywords.

Examples

The following is sample output from the show ip arp command:

```
Switch# show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Interface
Internet	1.1.1.1	-	7cb5.0157.0c00	eth-0-1
Internet	2.2.2.1	-	7cb5.0157.0c00	eth-0-2
Internet	3.3.3.1	-	7cb5.0157.0c00	eth-0-3
Internet	10.0.20.1	-	7cb5.0157.0c00	eth-0-10
Internet	10.0.20.254	-	0000.5e00.0101	eth-0-10

Related Commands

clear ip arp

4.1.12 show ip arp summary

Command Purpose

To display the total number of Address Resolution Protocol (ARP) table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router, use the show ip arp summary command in privileged EXEC mode.

Command Syntax

```
show ip arp ( vrf VRF-NAME | ) summary
```

Parameter	Parameter Description	Parameter Value
	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the vrf-name argument	
vrf VRF-NAME		String with up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display high-level statistics about the ARP table entries:

Examples

The following is sample output from the show ip arp summary command:

```
Switch# show ip arp summary
```

```
Gratuitous ARP learning is disabled
2 IP ARP entries, with 0 of them incomplete
(Static:1, Dynamic:0, Interface:1)
ARP Pkt Received is: 0
ARP Pkt Send number is: 1
ARP Pkt Discard number is: 0
```

Related Commands

clear ip arp statistics

4.1.13 debug arp

Command Purpose

To turn on the ARP debug, use debugs arp command in EXEC mode. To turn off the ARP debug, use the no form of this command.

Command Syntax

```
debug arp ( vrf VRF-NAME | )
```

Parameter	Parameter Description	Parameter Value
vrf VRF-NAME	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the vrf-name argument	String with up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to debug ARP packets received and send; also for debug ARP entry creating, updating and deleting.

Examples

The following is sample output from the debug arp command:

```
Switch# debug arp
```

```
Sep  7 03:34:08 SWITCH ARP-7: IP ARP: creating entry for IP address: 7.7.7.7, hw: e64d. 0445. df00
Sep  7 03:34:08 SWITCH ARP-7: IP ARP: send req src 7.7.7.7 e64d. 0445. df00, dst 7.7.7.7 eth-0-1
```

Related Commands

show debugging arp

4.1.14 show debugging arp

Command Purpose

To display the debugging status of ARP, use the show debugging arp command in EXEC mode.

Command Syntax

```
show debugging arp ( vrf VRF-NAME | )
```

Parameter	Parameter Description	Parameter Value
vrf VRF-NAME	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the vrf-name argument	String with up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the debugging status of ARP.

Examples

The following is sample output from the show debugging arp command:

```
Switch# show debugging arp
```

```
ARP debugging status:
```

```
ARP packet debugging is on
```

Related Commands

debug arp

4.1.15 proxy-arp enable**Command Purpose**

The switch uses proxy ARP to help hosts determine MAC addresses of hosts on other networks or subnets.

To enable proxy Address Resolution Protocol (ARP) on an interface, use the proxy-arp enable command in interface configuration mode.

To disable proxy ARP on the interface, use the no form of this command.

Command Syntax

proxy-arp enable

Command Mode

Interface Configuration

Default

Proxy ARP is disabled by default.

Usage

When proxy ARP is disabled, a device will respond to ARP requests received on its interface only if the target IP address is the same as its IP address.

Examples

The following example enables proxy ARP on interface eth-0-1:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#no shutdown
Switch(config-if)#ip address 1.1.1.1/24
Switch(config-if)# proxy-arp enable
```

Related Commands

local-proxy-arp enable

4.1.16 local-proxy-arp enable

Command Purpose

The local proxy ARP feature allow the L3 Device to response ARP request whose ARP Target address is in the same subnet the as the ARP request comes from (No Routing is required).

To enable local proxy Address Resolution Protocol (ARP) on an interface, use the local-proxy-arp enable command in interface configuration mode.

To disable proxy ARP on the interface, use the no form of this command.

Command Syntax

local-proxy-arp enable
no local-proxy-arp enable

Command Mode

Interface Configuration

Default

Local proxy ARP is disabled by default.

Usage

Internet Control Message Protocol (ICMP) redirects are disabled on interfaces when the local proxy ARP feature is enabled. The main condition we need to enable local ARP proxy is that the switch enables port isolate.

Examples

The following example enables local proxy ARP on interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 1.1.1.1/24
Switch(config-if)# local-proxy-arp enable
```

Related Commands

proxy-arp enable

4.1.17 gratuitous-arp-learning enable

Command Purpose

To enable the gratuitous Address Resolution Protocol (ARP) control on the router, use the `gratuitous-arp-learning enable` command in global configuration mode. To disable the ARP control, use the `no` form of this command.

Command Syntax

```
gratuitous-arp-learning enable
no gratuitous-arp-learning enable
```

Command Mode

Global Configuration

Default

Gratuitous ARP learning is disabled by default.

Usage

None

Examples

The following example enables gratuitous ARP learning on interface eth-0-1:

```
Switch# configure terminal
Switch(config)# gratuitous-arp-learning enable
```

Related Commands

show ip arp summary

4.1.18 gratuitous-arp send interval

Command Purpose

To config the gratuitous ARP send interval, use the no form of this command to recover to default.

Command Syntax

arp gratuitous-arp send interval *SECONDS*

no arp gratuitous-arp send interval

Parameter	Parameter Description	Parameter Value
SECONDS	The interval in seconds to send gratuitous ARP	1-86400 seconds

Command Mode

Interface Configuration

Default

60 seconds

Usage

None

The following example config gratuitous ARP send interval on interface eth-0-1:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#no shutdown
Switch(config-if)#ip address 1.1.1.1/24
Switch(config-if)#arp gratuitous-arp send interval 80
```

Related Commands

arp gratuitous-arp send enable

4.1.19 gratuitous-arp send enable

Command Purpose

To enable the gratuitous ARP send on the interface.

Command Syntax

arp gratuitous-arp send enable

no arp gratuitous-arp send enable

Command Mode

Interface Configuration

Default

Disbale

Usage

None

Examples

The following example enable gratuitous ARP on interface eth-0-1:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#no shutdown
Switch(config-if)#ip address 1.1.1.1/24
Switch(config-if)#arp gratuitous-arp send enable
```

Related Commands

arp gratuitous-arp send interval

4.2 DHCP Client Commands

4.2.1 ip address dhcp

Command Purpose

To acquire an IP address from Dynamic Host Configuration Protocol(DHCP), use the ip address dhcp command in interface configuration mode.

To disable the function, use the no form of this command.

Command Syntax

```
ip address dhcp
```

```
no ip address dhcp
```

Command Mode

Interface Configuration

Default

DHCP Client is not enabled on interface.

Usage

Once this command was enabled on an UP interface, it will acquire IP address immediately, otherwise the DHCP function of the interface will be in SUSPEND status.

The no ip address dhcp command will send a DHCPRELEASE message to server and remove any IP address.

Examples

The following example shows how to enable dhcp client function:

```
Switch# configure terminal
```

```
Switch(config-if)# ip address dhcp
```

The following example shows how to disable dhcp client function:

```
Switch# configure terminal
```

```
Switch(config-if)# no ip address dhcp
```

Related Commands

dhcp client request

dhcp client client-id

dhcp client class-id

dhcp client lease

dhcp client hostname

management ip address dhcp

show dhcp client

4.2.2 management ip address dhcp

Command Purpose

To acquire an IP address for management interface from by DHCP, use the management IP address dhcp command in global configuration mode.

To disable the function, use the no form of this command.

Command Syntax

management ip address dhcp

no management ip address dhcp

Command Mode

Global Configuration

Default

DHCP Client is not enabled on management interface.

Usage

Use this command like IP address dhcp.

Examples

The following example shows how to enable dhcp client function on management interface:

```
Switch# configure terminal
```

```
Switch(config)# management ip address dhcp
```

The following example shows how to disable dhcp client function on management interface:

```
Switch# configure terminal
Switch(config)# no management ip address dhcp
```

Related Commands

show dhcp client

4.2.3 dhcp client request

Command Purpose

To request configuration parameters by DHCP, use the dhcp client request command in interface configuration mode. To cancel the request, use the no form of this command.

Command Syntax

dhcp client request (router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific)

no dhcp client request (router | static-route | classless-static-route | classless-static-route-ms | tftp-server-address | dns-nameserver | domain-name | netbios-nameserver | vendor-specific)

Parameter	Parameter Description	Parameter Value
router	Default router option (3)	-
static-route	Static route option (33)	-
classless-static-route	Classless static route option (121)	-
classless-static-route-ms	Microsoft classless static route option (249)	-
tftp-server-address	TFTP server ip address option (150)	-
dns-nameserver	DNS name server option (6)	-
domain-name	Domain name option (15)	-
netbios-nameserver	NetBIOS name server option (44)	-
vendor-specific	Vendor specific option (43)	-

Command Mode

Interface Configuration

Default

static-route, classless-static-route, classless-static-route-ms, tftp-server-address and router is requested as default.

Usage

Use this command to request configuration from DHCP server. It can be typed many times with each option or one time with all options wanted. Note that when Option 249 coexist with option 121 then the option 121 should have high priority and option 249 should be ignored. when option 121 or option 249 coexist with option 33 then the option 33 should be ignored. This command should be issued before ip address dhcp command. If you issued ip address dhcp before, this command will take effect after next ip address dhcp command.

Examples

The following example shows how to request dhcp option static-route and tftp-server-address:

```
Switch# configure terminal
Switch(config-if)# no management ip address dhcp
```

The following example shows how to request dhcp option router:

```
Switch# configure terminal
Switch(config-if)# dhcp client request router
```

The following example shows how to cancel request of dhcp option router:

```
Switch# configure terminal
Switch(config-if)# no dhcp client request router
```

The following example shows how to request tftp server address:

```
Switch# configure terminal
Switch(config-if)# dhcp client request static-route tftp-server-address
```

Related Commands

ip address dhcp

4.2.4 dhcp client client-id

Command Purpose

To specify a client-id used by DHCP server and client for identifying a client, use the dhcp client client-id command in interface configuration mode.

To remove this configuration, use the no form of this command.

Command Syntax

dhcp client client-id (*ascii WORD* | *hex HEX-STRING* | *IFVLAN* | *IFAGG* | *IFPHYSICAL*)

no dhcp client client-id

Parameter	Parameter Description	Parameter Value
ascii	ASCII type	-
WORD	Client-ID as ascii string	String with up to 64 characters
hex	Hex type	-
HEX-STRING	Class-ID in hex string	String with up to 64 characters

Parameter	Parameter Description	Parameter Value
IFVLAN	Vlan interface's name	1-4094
IFAGG	Aggregation interface's name	-
IFPHYSICAL	Physical interface's name	-

Command Mode

Interface Configuration

Default

The default client-id, format of which is like "switch-HWADDR-IFNAME", will be used.

Usage

This command should be issued before IP address dhcp command. If you issued IP address dhcp before, this command will take effect after next IP address dhcp command.

Examples

The following example shows how to specify a client-id for an interface:

```
Switch# configure terminal
Switch(config-if)# dhcp client client-id ascii switch-client
```

The following example shows how to delete client-id set before:

```
Switch# configure terminal
Switch(config-if)# no dhcp client client-id
```

Related Commands

ip address dhcp

4.2.5 dhcp client class-id

Command Purpose

To specify a class-id for DHCP server and client, use the dhcp client class-id command in interface configuration mode. To remove this configuration, use the no form of this command.

Command Syntax

dhcp client class-id (*WORD* | hex *HEX-STRING*)

no dhcp client class-id

Parameter	Parameter Description	Parameter Value
WORD	Client-ID as ascii string	-
hex	Hex type	-
HEX-STRING	Class-ID in hex string	-

Command Mode

Interface Configuration

Default

No class-id is set.

Usage

Class-id used by DHCP clients to optionally identify the type and configuration of a DHCP client. Vendors and sites may choose to define specific class identifiers to convey particular configuration or other identification information about a client. This command should be issued before ip address dhcp command. If you issued ip address dhcp before, this command will take effect after next ip address dhcp command.

Examples

The following example shows how to specify class-id for an interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp client class-id acsii switch
```

The following example shows how to delete class-id set before:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no dhcp client class-id
```

Related Commands

ip address dhcp

4.2.6 dhcp client lease

Command Purpose

To configure the duration of the lease for an IP address request by DHCP client, use the dhcp client lease command in interface configuration mode.

To remove the configuration, use the no form of this command.

Command Syntax

dhcp client lease *DAYS* (*HOURS* (*MINUTES* |) |) | infinite)

no dhcp client lease

Parameter	Parameter Description	Parameter Value
DAYS	The number of days in lease	0-365
HOURS	The number of hours in the lease.	0-23
MINUTES	The number of minutes in the lease	0-59
infinite	infinite lease	-

Command Mode

Interface Configuration

Default

No lease is requested by client.

Usage

Use this command to specify the lease wanted by client, DHCP server may accept this request or ignore it. This command should be issued before ip address dhcp command. If you issued ip address dhcp before, this command will take effect after next ip address dhcp command.

Examples

The following example shows how to specify lease 20 minutes for dhcp client:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp client lease 0 0 20
```

The following example shows how to remove the lease set before:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no dhcp client lease
```

Related Commands

ip address dhcp

4.2.7 dhcp client hostname

Command Purpose

To specify or modify the hostname sent in the DHCP message; use the `dhcp client hostname` command in interface configuration mode.
To remove the hostname, use the `no` form of this command.

Command Syntax

`dhcp client hostname WORD`

`no dhcp client hostname`

Parameter	Parameter Description	Parameter Value
WORD	Host name	String with up to 256 characters

Command Mode

Interface Configuration

Default

The host name in system will be used.

Usage

This command should be issued before `ip address dhcp` command. If you issued IP address `dhcp` before, this command will take effect after next IP address `dhcp` command.

Examples

The following example shows how to specify name of the host:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp client hostname switch
```

The following example shows how to remove the last set:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no dhcp client hostname
```

Related Commands

`ip address dhcp`

4.2.8 dhcp client default-router distance

Command Purpose

To specify the default router distance for the routes leased from DHCP server, use the dhcp client default-router distance command in global configuration mode. To remove the configuration, use the no form of this command.

Command Syntax

dhcp client default-router distance *METRIC*

no dhcp client default-router distance

Parameter	Parameter Description	Parameter Value
METRIC	The default metric of routes	1-255

Command Mode

Global Configuration

Default

The default value for the default metric is 254.

Usage

None

Examples

The following example shows how to set dhcp client default route metric as 233:

```
Switch# configure terminal
```

```
Switch(config)# dhcp client default-router distance 233
```

The following example shows how to use the default value of default route metric:

```
Switch# configure terminal
```

```
Switch(config)# no dhcp client default-router distance
```

Related Commands

ip address dhcp

4.2.9 dhcp client broadcast-flag

Command Purpose

To specify the broadcast-flag in the DHCP message, use the dhcp client broadcast-flag command in global configuration mode.

To remove this configuration, use the no form of this command.

Command Syntax

dhcp client broadcast-flag

no dhcp client broadcast-flag

Command Mode

Global Configuration

Default

Broadcast-flag will be set in DHCP message sent by client for request IP address.

Usage

This flag tell DHCP server that client can't receive unicast IP datagrams until been configured with an IP address. Thus server or relay agent will broadcast any messages to the client on the client's subnet.

Examples

The following example shows how to set broadcast-flag:

```
Switch# configure terminal
```

```
Switch(config)# dhcp client broadcast-flag
```

The following example shows how to delete broadcast-flag:

```
Switch# configure terminal
```

```
Switch(config)# no dhcp client broadcast-flag
```

Related Commands

ip address dhcp

4.2.10 debug dhcp client

Command Purpose

Use this command to turn on the debug switches of dhcp client module.

To restore the default, use the no form of this command

Command Syntax

debug dhcp client (events | error | dump | packet | all)

no debug dhcp client (events | error | dump | packet | all)

Parameter	Parameter Description	Parameter Value
events	Client events	-
error	Error DHCP message	-
packet	DHCP message fields	-
dump	Dump message in hex format	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.

Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcp client debug switches:

```
Switch# debug dhcp client all
```

Related Commands

terminal monitor

show logging buffer

4.2.11 show dhcp client

Command Purpose

To show information of dhcp client on one or all interfaces, use the show dhcp client command in privileged EXEC mode.

Command Syntax

show dhcp client (management | IFVLAN | IFAGG | IFPHYSICAL |) (verbose |)

Parameter	Parameter Description	Parameter Value
management	Management interface	-
IFVLAN	Vlan interface's name	1-4094
IFAGG	Aggregation interface's name	-
IFPHYSICAL	Physical interface's name	-
verbose	DHCP client verbose information	-

Command Mode

Privileged EXEC

Default

None

Usage

To see more detail information, add verbose at the last of command

Examples

The following example shows how to display DHCP client information on all interfaces:

```
Switch# show dhcp client verbose
```

```
DHCP client informations:
```

```
=====
```

```
vlan1 DHCP client information:
```

```
Current state: SELECT
```

```
Transaction ID: 0x3ac1c1c7
```

```
=====
```

```
eth-0-1 DHCP client information:
```

```
Current state: SELECT
```

```
Transaction ID: 0x2fd3f55b
```

Related Commands

ip address dhcp

4.2.12 show dhcp client statistics

Command Purpose

To show statistics of DHCP client, use the show dhcp client statistics command in privileged EXEC mode.

Command Syntax

```
show dhcp client statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to show the status of DHCP client, like DHCP packets counter.

Examples

The following example shows how to display DHCP packets statistics:

```
Switch# show dhcp client statistics
```

```
DHCP client packet statistics:
```

```
=====
DHCP OFFERS      received: 0
DHCP ACKs        received: 0
DHCP NAKs        received: 0
DHCP Others      received: 0
DHCP DISCOVER    sent: 0
DHCP DECLINE     sent: 0
DHCP RELEASE     sent: 0
DHCP REQUEST     sent: 0
DHCP packet send failed: 0
```

Related Commands

```
ip address dhcp
```

4.2.13 clear dhcp client statistics

Command Purpose

To clear statistics of dhcp client, use the clear dhcp client statistics command in privileged EXEC mode.

Command Syntax

```
clear dhcp client statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

This command will clear DHCP packet counter.

Examples

The following example shows how to clear statistics:

```
Switch# clear dhcp client statistics
```

Related Commands

```
ip address dhcp  
show dhcp client statistics
```

4.3 DHCP Relay Commands

4.3.1 dhcp relay

Command Purpose

To enable the DHCP relay service, use the dhcp relay command in global configuration mode.

To disable this function, use the no form of this command.

Command Syntax

dhcp relay

no dhcp relay

Command Mode

Global Configuration

Default

DHCP relay is disabled.

Usage

The DHCP service must be enabled with the dhcp service command before DHCP relay service can be used.

Examples

The following example shows how to enable DHCP relay agent:

```
Switch# configure terminal
Switch(config)# dhcp relay
```

Related Commands

service dhcp

4.3.2 dhcp-server (global)

Command Purpose

To create a DHCP server group, use the dhcp-server command in global configuration mode.

To remove a DHCP server group, use the no form of this command.

Command Syntax

dhcp-server *NUMBER SERVER-LIST*

no dhcp-server *NUMBER (SERVER-LIST |)*

Parameter	Parameter Description	Parameter Value
NUMBER	Number of the DHCP server group.	1-16
SERVER-LIST	The IP address list of the DHCP server.	1-16

Command Mode

Global Configuration

Default

No DHCP server group is defined.

Usage

This command is used to specify the remote DHCP server.

Examples

The following example shows how to configure dhcp-server group globally:

```
Switch# configure terminal
Switch(config)# dhcp-server 1 1.1.1.1 2.2.2.2 3.3.3.3
```

Related Commands

service dhcp

dhcp-server (interface)

4.3.3 dhcp-server (interface)**Command Purpose**

To add an interface into a DHCP server group, use the dhcp-server command in interface configuration mode.

To remove this interface from the DHCP server group, use the no form of this command.

Command Syntax

dhcp-server *NUMBER*

no dhcp-server

Parameter	Parameter Description	Parameter Value
NUMBER	Number of the DHCP server group.	1-16

Command Mode

Interface Configuration

Default

No DHCP server group is configured for the interface.

Usage

This command is used to specify DHCP server group which is configured by the command `dhcp-server` in global mode.

Examples

The following example shows how to configure `dhcp-server` group for interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp-server 1
```

Related Commands

`service dhcp`

4.3.4 dhcp relay information check

Command Purpose

To enable validation of relay agent information option in forwarded reply messages, use the `dhcp relay information check` command in global configuration mode.

To disable an information check, use the `no` form of this command.

Command Syntax

```
dhcp relay information check
no dhcp relay information check
```

Command Mode

Global Configuration

Default

The validation of relay agent information is enabled. Invalid messages are dropped.

Usage

None

Examples

The following example shows how to enable validation of relay agent information:

```
Switch# configure terminal
Switch(config)# dhcp relay information check
```

Related Commands

dhcp relay information option

4.3.5 dhcp relay information option

Command Purpose

To enable the system to insert a DHCP relay agent information option in forwarded request messages to a DHCP server, use the dhcp relay information option command in global configuration mode. To disable inserting relay information, use the no form of this command.

Command Syntax

```
dhcp relay information option
no dhcp relay information option
```

Command Mode

Global Configuration

Default

No relay agent information is inserted.

Usage

The dhcp relay information option command automatically adds the circuit identifier suboption and the remote ID suboption to the DHCP relay agent information option (also called option 82).

Examples

The following example shows how to enable inserting of dhcp relay information option:

```
Switch# configure terminal
Switch(config)# dhcp relay information option
```

Related Commands

dhcp relay information check

dhcp relay information policy

4.3.6 dhcp relay information policy

Command Purpose

To configure the information re-forwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information), use the dhcp relay information policy command in global configuration.

To restore the default relay information policy, use the no form of this command.

Command Syntax

dhcp relay information policy (drop | keep | replace)

no dhcp relay information policy

Parameter	Parameter Description	Parameter Value
drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present	-
keep	Indicates that existing information is left unchanged on the DHCP relay agent	-
replace	Indicates that existing information is overwritten on the DHCP relay agent	-

Command Mode

Global Configuration

Default

The DHCP relay won't change existing relay information.

Usage

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, this message will be forwarded with the relay information from the previous relay agent untouched.

Examples

The following example shows how to configure policy of dhcp relay information :

```
Switch# configure terminal
Switch(config)# dhcp relay information policy drop
```

Related Commands

dhcp relay information option
dhcp relay information policy

4.3.7 dhcp relay information policy (interface)

Command Purpose

If Option 82 policy is configured on interface, the content of option 82 in packet will be processed according to the interface policy, otherwise it will be processed according to global policy.

Command Syntax

dhcp relay information policy (drop | keep | replace)
no dhcp relay information policy

Parameter	Parameter Description	Parameter Value
drop	Directs the DHCP relay agent to discard messages with existing relay information if the relay information option is already present	-
keep	Indicates that existing information is left unchanged on the DHCP relay agent	-
replace	Indicates that existing information is overwritten on the DHCP relay agent	-

Command Mode

Interface Configuration

Default

No Option 82 policy is configured on interface.

Usage

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, this message will be forwarded with the relay information from the previous relay agent untouched.

Examples

The following example shows how to configure policy of dhcp relay information :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp relay information policy drop
```

Related Commands

dhcp relay information option

4.3.8 dhcp relay information trust-all

Command Purpose

To configure all interfaces as trusted sources of the DHCP relay agent information option, use the dhcp relay information trust-all command in global configuration mode. To restore these interfaces to their default behavior, use the no form of this command.

Command Syntax

dhcp relay information trust-all

no dhcp relay information trust-all

Command Mode

Global Configuration

Default

All interfaces on the switch are considered entrusted.

Usage

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the DHCP relay agent will discard the packet. If the `dhcp relay information trust-all` command is configured globally, the DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the `dhcp-server` command as in normal DHCP relay operation.

Examples

The following example shows how to configure `dhcp relay information trust` globally:

```
Switch# configure terminal
Switch(config)# dhcp relay information trust-all
```

Related Commands

`dhcp relay information trusted`

4.3.9 dhcp relay information trusted

Command Purpose

To configure an interface as a trusted source of DHCP relay agent information option, use the `dhcp relay information trusted` command in interface configuration mode. To restore the interface to the default behavior, use the `no` form of the command.

Command Syntax

`dhcp relay information trusted`

`no dhcp relay information trusted`

Command Mode

Interface Configuration

Default

All interfaces on the router are considered entrusted.

Usage

By default, if the gateway address is set to all zeros in the DHCP packet and the relay information option is already present in the packet, the DHCP relay agent will discard the packet. If the `dhcp relay information trusted` command is configured globally, the DHCP relay agent will not discard the packet even if the gateway address is set to all zeros. Instead, the received DHCPDISCOVER or DHCPREQUEST messages will be forwarded to the addresses configured by the `dhcp-server` command as in normal DHCP relay operation.

Examples

The following example shows how to configure an interface as trusted source of dhcp relay information:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp relay information trusted
```

Related Commands

dhcp relay information trust-all

4.3.10 dhcp relay gateway

Command Purpose

To configure the DHCP relay agent address of DHCP packets, use this command in interface configuration mode.

To restore the interface to the default behavior, use the no form of the command.

Command Syntax

dhcp relay gateway *A.B.C.D*

no dhcp relay gateway

Command Mode

Interface Configuration

Default

Default relay agent address is used in DHCP packet.

Usage

None

Examples

The following example shows how to configure DHCP relay agent address of DHCP packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp relay gateway 10.10.10.1
```

Related Commands

dhcp-server (interface)

4.3.11 dhcp relay address cycle

Command Purpose

Use "dhcp relay address cycle" command to enable DHCP relay cycle feature.

Use "no dhcp relay address cycle" to disable the feature.

Command Syntax

dhcp relay address cycle
no dhcp relay address cycle

Command Mode

Global Configuration

Default

DHCP relay cycle is disabled by default.

Usage

This command is used for DHCP relay. When more than one DHCP servers are configured on a DHCP relay device, relay device should send DHCP DISCOVER packets to all servers by default. In this way, the servers should deal with too much packet and might be overload. To resolve this problem use this command to enable DHCP relay cycle. After configure this command, DHCP relay device send to only one server when it receive the DHCP DISCOVER packet, and it will change a server to send packet every time after it sent one. Use this method to make all servers to achieve load balance.

Examples

Enable DHCP relay cycle feature :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp relay address cycle
```

Related Commands

None

4.3.12 service dhcp

Command Purpose

To enable the Dynamic Host Configuration Protocol (DHCP) snooping and relay agent features on your router, use the service dhcp command in global configuration mode.

To disable the DHCP snooping and relay agent features, use the no form of this command.

Command Syntax

service dhcp enable

service dhcp disable

Command Mode

Global Configuration

Default

DHCP service is disabled globally.

Usage

Only the main DHCP service is enabled by the service dhcp command, can other DHCP services be used, such as dhcp relay or dhcp snooping.

Examples

The following example shows how to enable DHCP service globally:

```
Switch# configure terminal
```

```
Switch(config)# service dhcp enable
```

The following example shows how to disable DHCP service globally:

```
Switch# configure terminal
```

```
Switch(config)# service dhcp disable
```

Related Commands

dhcp relay
dhcp snooping

4.3.13 debug dhcp relay

Command Purpose

Use this command to turn on the debug switches of dhcp relay module.

To restore the default, use the no form of this command

Command Syntax

debug dhcp relay (events | error | dump | packet | all)

no debug dhcp relay (events | error | dump | packet | all)

Parameter	Parameter Description	Parameter Value
events	Relay events	-
error	Error DHCP message	-
packet	DHCP message fields	-
dump	Dump message in hex format	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.

Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcp relay debug switches:

```
Switch# debug dhcp relay all
```

Related Commands

terminal monitor
show logging buffer

4.3.14 show dhcp-server

Command Purpose

To display the DHCP server groups, use the show dhcp-server command in privileged EXEC mode.

Command Syntax

show dhcp-server

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display all the DHCP server groups configured with command dhcp-server in global mode.

Examples

The following example shows how to display dhcp-server group information:

```
Switch# show dhcp-server
```

DHCP server group information:

```
=====
```

group 1 ip address list:

```
[1] 1.1.1.1  
[2] 2.2.2.2  
[3] 3.3.3.3  
[4] 4.4.4.4  
[5] 5.5.5.5  
[6] 6.6.6.6  
[7] 7.7.7.7  
[8] 8.8.8.8
```

Related Commands

dhcp-server (global)

4.3.15 show dhcp relay interfaces

Command Purpose

To display to which dhcp-server group the interface belongs, use the show dhcp relay interfaces command in privileged EXEC mode.

Command Syntax

show dhcp relay interfaces

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the interface which is confined DHCP relay.

Examples

The following example shows how to display dhcp relay interfaces information:

```
Switch# show dhcp relay interfaces
```

```
List of DHCP relay enabled interface(s):
```

```
DHCP relay service status: enabled
```

```
Interface Name          DHCP server group
```

```
=====
```

eth-0-1	1

Related Commands

show dhcp-server

4.3.16 show dhcp relay information config

Command Purpose

To display the DHCP relay information configurations, use the show dhcp relay information config command in privileged EXEC mode.

Command Syntax

```
show dhcp relay information config
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCP relay.

Examples

The following example shows how to display dhcp relay configuration:

```
Switch# show dhcp relay information config
```

```
DHCP relay agent information configuration:
```

```
=====
no dhcp relay information option
dhcp relay information check
dhcp relay information policy keep
```

Related Commands

```
dhcp relay information option
```

4.3.17 show dhcp relay information trusted-sources

Command Purpose

To display all interfaces configured to be a trusted source for the DHCP relay information option, use the show dhcp relay information trusted-sources command in privileged EXEC mode.

Command Syntax

show dhcp relay information trusted-sources

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display all interfaces configured to be a trusted source for DHCP relay.

Examples

The following example shows how to display dhcp relay information trusted-sources:

```
Switch# show dhcp relay information trusted-sources
```

List of trusted sources of relay agent information option:

```
=====
All interfaces are trusted source of relay agent information option
```

Related Commands

dhcp relay information trusted

4.3.18 show dhcp relay statistics

Command Purpose

To display the statistics of DHCP packets relayed by the switch, use the show dhcp relay statistics command in privileged EXEC mode.

Command Syntax

show dhcp relay statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display detail DHCP statistics which dealt by the switch.

Examples

The following example shows how to display dhcp relay statistics:

```
Switch# show dhcp relay statistics
```

DHCP relay packet statistics:

```
=====
Client relayed packets: 101
Server relayed packets: 88
Client error packets: 0
Server error packets: 0
Bogus GIADDR drops: 15
Bad circuit ID packets: 0
Corrupted agent options: 0
Missing agent options: 0
Missing circuit IDs: 0
```

Related Commands

clear dhcp relay statistics

4.3.19 clear dhcp relay statistics

Command Purpose

To clear the statistics of DHCP packets relayed by the switch, use the clear dhcp relay statistics command in privileged EXEC mode.

Command Syntax

clear dhcp relay statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear detail DHCP statistics which dealt by the switch.

Examples

The following example shows how to clear dhcp relay statistics:

```
Switch# clear dhcp relay statistics
```

Related Commands

show dhcp relay statistics

4.4 DHCP Server Commands

4.4.1 service dhcp

Command Purpose

To enable or disable the DHCP snooping, server and relay agent features on your router, use the service dhcp command in global configuration mode.

To disable these functions, use the no form of this command.

Command Syntax

```
service dhcp enable  
service dhcp disable
```

Command Mode

Global Configuration

Default

DHCP service is disabled.

Usage

Only the main DHCP service is enabled by the service dhcp command, can other DHCP services be used, such as dhcp relay, dhcp server and dhcp snooping.

Examples

The following example enables dhcp service:

```
Switch# configure terminal
```

```
Switch(config)# service dhcp enable
```

The following example disables dhcp service:

```
Switch# configure terminal
```

```
Switch(config)# service dhcp disable
```

Related Commands

dhcp server

dhcp relay

dhcp snooping

4.4.2 dhcp-server (global)

Command Purpose

To enable the DHCP server service, use the dhcp server command in global configuration mode.

To disable this function, use the no form of this command.

Command Syntax

dhcp server

no dhcp server

Command Mode

Global Configuration

Default

DHCP server is disabled.

Usage

The DHCP service must be enabled with the `dhcp server` command before DHCP server service can be used.

Examples

The following is sample output from the `dhcp server` command:

```
Switch# configure terminal
Switch(config)# dhcp server
```

Related Commands

`service dhcp`

`dhcp-server (interface)`

4.4.3 dhcp-server (interface)

Command Purpose

To specify a L3 interface to act as a DHCP Server, use the `dhcp server` command in interface configuration mode. To remove the specification, use the `no` form of this command.

Command Syntax

`dhcp server enable`

`dhcp server disable`

Parameter	Parameter Description	Parameter Value
enable	Specify a L3 interface to act as a DHCP server	-
disable	Remove DHCP server on a L3 interface	-

Command Mode

Interface Configuration

Default

Neither DHCP server nor DHCP relay is specified.

Usage

This command is used to specify a L3 interface to act as a DHCP Server.

Examples

The following is sample output from the dhcp server command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp server enable
```

Related Commands

service dhcp

dhcp server(global)

4.4.4 dhcp ping packets

Command Purpose

To configure how many ping packets that are sent before assigning the address to a requesting client, use the dhcp ping packets command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

dhcp ping packets *NUMBER*

no dhcp ping packets

Parameter	Parameter Description	Parameter Value
NUMBER	Specify the number of ping packets that are sent before assigning the address to a requesting client	0-10

Command Mode

Global Configuration

Default

The default value is one packet.

Usage

The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Examples

The following is sample output from the dhcp ping packets command:

```
Switch# configure terminal
Switch(config)# dhcp ping packets 10
```

Related Commands

service dhcp
dhcp ping timeout

4.4.5 dhcp ping timeout

Command Purpose

To configure how long a DHCP server waits for a ping reply from an address pool; use the dhcp ping timeout command in interface configuration mode.

To restore the default value, use the no form of this command.

Command Syntax

dhcp ping timeout *NUMBER*

no dhcp ping timeout

Parameter	Parameter Description	Parameter Value
NUMBER	Specifies how long to wait for a ping reply in seconds.	1-10 seconds

Command Mode

Global Configuration

Default

The default value is waiting for one second.

Usage

The DHCP server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

Examples

The following is sample output from the dhcp ping timeout command:

```
Switch# configure terminal
Switch(config)# dhcp ping timeout 3
```

Related Commands

service dhcp

dhcp ping packets

4.4.6 dhcp pool

Command Purpose

To configure the information reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information), use the dhcp relay information policy command in global configuration.

To restore the default relay information policy, use the no form of this command.

Command Syntax

dhcp pool *WORD*

no dhcp pool *WORD*

Parameter	Parameter Description	Parameter Value
		1) the length range should be [1, 32)
WORD	WORD: The name of a DHCP pool	2) The characters can only include [0-9a-zA-Z.-_] 3) The string must starting with alphabetic, ending with alphanumeric or digit

Command Mode

Global Configuration

Default

The default value is DHCP address pools are not configured.

Usage

During execution, the configuration mode changes to DHCP pool configuration mode, identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, like the IP subnet number and default router list.

Examples

The following is sample output from the dhcp pool command:

```
Switch# configure terminal
Switch(config)# dhcp pool pool1
```

Related Commands

service dhcp

dhcp select

static-bind

dhcp excluded-address

network (DHCP)

4.4.7 static-bind

Command Purpose

To specify an address binding mapping between the IP address and MAC address of a client, use the static-bind pool configuration command. To remove the address binding mapping, use the no form of this command.

Command Syntax

static-bind ip-address *IP_ADDR/IP_MASK_LEN* (mac-address *MAC_ADDR* | client-identifier (*ascii WORD* | *hex HEX_STRING*))

static-bind ip-address *IP_ADDR IP_ADDR_MASK* (mac-address *MAC_ADDR* | client-identifier (*ascii WORD* | *hex HEX_STRING*))

no static-bind

Parameter	Parameter Description	Parameter Value
IP_ADDR	IP address.	IPv4 Address
IP_ADDR_MASK	IP-address-type mask	IPv4 Address
IP_MASK_LEN	Prefix length for the ip address.	1-32

Parameter	Parameter Description	Parameter Value
mac-address MAC_ADDR	the hardware address of a DHCP client.	MAC Address
ascii WORD	the client id as ascii string	String with up to 63 characters
hex HEX_STRING	the client id as hex string	String with up to 126 characters

Command Mode

DHCP pool Configuration

Default

The default value is none address binding mapping specified.

Usage

You can only configure one manual binding per host pool.

Examples

The following is sample output from the static-bind command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# static-bind ip 10.10.10.10/24 mac-address 0012.2222.2222
```

Related Commands

dhcp pool

4.4.8 dns-server address

Command Purpose

To specify the DNS IP servers available to a DHCP client, use the dns-server DHCP pool configuration command. To remove the DNS server list, use the no form of this command.

Command Syntax

dns-server *A.B.C.D* (*A.B.C.D*... *A.B.C.D*)

no dns-server

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.	IPv4 Address
A.B.C.D... A.B.C.D (Optional)	Specifies up to eight addresses in the command line.	IPv4 Address

Command Mode

DHCP pool Configuration

Default

The default value is none DNS IP servers specified.

Usage

You can specify up to eight servers in the list, Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following is sample output from the dns-server command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# dns-server 1.1.1.1 2.2.2.2
```

Related Commands

dhcp pool

4.4.9 domain-name

Command Purpose

To specify the domain name for a DHCP client, use the domain-name DHCP pool configuration command. To remove the domain name, use the no form of this command.

Command Syntax

domain-name *WORD*

no domain-name

Parameter	Parameter Description	Parameter Value
WORD	specify a domain name suffix in each DHCP address pool on the DHCP server for the clients.	1) The length range should be [1, 64)
		2) The characters can only include [0-9a-zA-Z.-_], specify a domain name suffix in each DHCP address pool on the DHCP server for the clients.
		1) The length range should be [1, 64) 2) The characters can only include [0-9a-zA-Z.-_], 3) The string must starting with alphabetic, ending with alphanumeric or digit

Command Mode

DHCP pool Configuration

Default

The default value is none domain-name specified.

Usage

You can specify a domain name suffix in each DHCP address pool on the DHCP server for the clients. With this suffix assigned, the client needs only input part of a domainname, and the system will add the domain name suffix for name resolution.

Examples

The following is sample output from the domain-name command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# domain-name switch.org
```

Related Commands

dhcp pool

4.4.10 bootfile-name

Command Purpose

To specify the name of the default boot image for a DHCP client, use the bootfile-name DHCP pool configuration command. To delete the boot image name, use the no form of this command.

Command Syntax

bootfile-name *WORD*

no bootfile-name

Parameter	Parameter Description	Parameter Value
		1) The length range should be [1, 64)
		2) The characters can only include [0-9a-zA-Z.-_],
		Specifies the name of the file that is used as a boot image.
WORD	Specifies the name of the file that is used as a boot image.	1) The length range should be [1, 64)
		2) The characters can only include [0-9a-zA-Z.-_],
		3) The string must starting with alphabetic, ending with alphanumeric or digit

Command Mode

DHCP pool Configuration

Default

The default value is none boot file specified.

Usage

This task is to specify the IP address and name of a TFTP server and the bootfile name in the DHCP address pool. The DHCP clients use these parameters to contact the TFTP server, requesting the configuration file used for system initialization, which is called autoconfiguration.

Examples

The following example specifies dhclient_startup_config as the name of the boot file:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# bootfile dhclient_startup_config
```

Related Commands

dhcp pool

tftp-server-address

4.4.11 tftp-server-address

Command Purpose

To configure the tftp server in the boot process of a DHCP client, use the tftp-server-address DHCP pool configuration command. To remove the boot server list, use the no form of this command.

Command Syntax

tftp-server-address *A.B.C.D* (*A.B.C.D... A.B.C.D*)

no tftp-server-address

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the address of the tftp server address in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server. One address is required, although you can specify up to eight addresses in one command line.	IPv4 Address
A.B.C.D... A.B.C.D (Optional)	Specifies up to eight address in the command line.	IPv4 Address

Command Mode

DHCP pool Configuration

Default

The default value is none tftp-server-address specified.

Usage

You can specify up to eight servers in the list, Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following is sample output from the tftp-server-address command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# tftp-server-address 1.1.1.1 2.2.2.2
```

Related Commands

dhcp pool

bootfile-name

4.4.12 gateway address

Command Purpose

To specify the default router list for a DHCP client, use the gateway DHCP pool configuration command. To remove the default router list, use the no form of this command.

Command Syntax

gateway *A.B.C.D* (*A.B.C.D*... *A.B.C.D*)

no gateway

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.	IPv4 Address
A.B.C.D... A.B.C.D (Optional)	Specifies up to eight addresses in the command line.	IPv4 Address

Command Mode

DHCP pool Configuration

Default

The default value is none gateway servers specified.

Usage

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 is the most preferred router, address2 is the next most preferred router, and so on).

Examples

The following is sample output from the gateway command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# gateway 1.1.1.1 2.2.2.2
```

Related Commands

dhcp pool

4.4.13 netbios-name-server

Command Purpose

To specify the default router list for a DHCP client, use the netbios-name-server DHCP pool configuration command. To remove the default router list, use the no form of this command.

Command Syntax

netbios-name-server *A.B.C.D* (*A.B.C.D... A.B.C.D*)

no netbios-name-server

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.	IPv4 Address
A.B.C.D... A.B.C.D (Optional)	Specifies up to eight addresses in the command line.	IPv4 Address

Command Mode

DHCP pool Configuration

Default

The default value is none NetBIOS WINS name servers specified.

Usage

You can specify up to eight NetBIOS WINS name servers in the list. NetBIOS WINS name servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Examples

The following is sample output from the netbios-name-server command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# netbios-name-server 1.1.1.1 2.2.2.2
```

Related Commands

dhcp pool

4.4.14 netbios-node-type

Command Purpose

To configure the NetBIOS node type for DHCP clients, use the netbios-node-type DHCP pool configuration command.

To remove the NetBIOS node type, use the no form of this command.

Command Syntax

netbios-node-type [b-node | p-node | m-node | h-node]

no netbios-node-type

Parameter	Parameter Description	Parameter Value
b-node	Broadcast	-
p-node	Peer-to-peer	-
m-node	Mixed	-
h-node	Hybrid (recommended)	-

Command Mode

DHCP pool Configuration

Default

The default value is none NetBIOS node type specified.

Usage

You can specify the NetBIOS node type for a DHCP address pool which is used to specify the NetBIOS node type for a DHCP Client.

Examples

The following is sample output from the netbios-node-type command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# netbios-node-type h-node
```

Related Commands

dhcp pool

4.4.15 network

Command Purpose

To configure the subnet number and mask for a DHCP address pool on a DHCP Server, use the network DHCP pool configuration command.

To remove the subnet number and mask, use the no form of this command.

Command Syntax

network [ip-address wildcard-mask | ip-address/prefix-length]

no network

Parameter	Parameter Description	Parameter Value
ip-address	IP address.	IPv4 Address
wildcard-mask	IP-address-type mask that includes "don't care" bits.	IPv4 Address
prefix-length	Prefix length for the network.	0-32

Command Mode

DHCP pool Configuration

Default

The default value is none subnet number and mask specified.

Usage

This command is valid for DHCP subnetwork address pools only. The DHCP server assumes that all host addresses are available. The system administrator can exclude subsets of the address space by using the `ip dhcp excluded-address` command. Network for one pool can't be the same with other pool's network and can't configure manual bindings within the same pool that is configured with the `network` command.

Examples

The following is sample output from the `netbios-node-type` command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# network 1.1.1.0/24
```

Related Commands

`dhcp pool`

4.4.16 Lease

Command Purpose

To configure the duration of the lease for an IP address that is assigned from a DHCP Server to a DHCP client, use the `lease DHCP pool` configuration command. To restore the default value, use the `no` form of this command.

Command Syntax

`lease DAYS ( HOURS ( MINUTES | ) | )`

`no lease`

Parameter	Parameter Description	Parameter Value
DAYS	Specifies the duration of the lease in numbers of days.	0-365 days
HOURS (Optional)	Specifies the number of hours in the lease. A days value must be supplied before you can configure an hours value.	0-23 hours

Parameter	Parameter Description	Parameter Value
MINUTES (Optional)	Specifies the number of minutes in the lease. A day's value and an hours value must be supplied before you can configure a minute's value.	0-59 minutes

Command Mode

DHCP pool Configuration

Default

The default value is one day.

Usage

N/A

Examples

The following example shows a two-day lease:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# lease 2
```

The following example shows a one-day and two-hour lease:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# lease 1 2
```

The following example shows a thirty-minute lease:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# lease 0 0 30
```

Related Commands

dhcp pool

4.4.17 Option

Command Purpose

To configure DHCP Server options, use the option DHCP pool configuration command.

To remove the options, use the no form of this command.

Command Syntax

```
option { code [ ascii ascii-string | hex hex-string | ip-address ip-address ] }
```

```
no option [ code ]
```

Parameter	Parameter Description	Parameter Value
code	Specifies the DHCP option code.	2-254
ascii-string	Specifies an NVT ASCII character string. ASCII character strings that contain white space must be delaminated by quotation marks.	String with up to 63 characters
hex-string	Specifies dotted-hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digitse.	String with up to 126 characters
ip-address	Specifies an IP address.	IPv4 Address

Command Mode

DHCP pool Configuration

Default

The default value is none DHCP option specified.

Usage

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, Dynamic Host Configuration Protocol.

Examples

The following is sample output from the option command:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# option 72 ip-address 10.10.10.10 11.11.11.11
```

Related Commands

dhcp pool

4.4.18 dhcp excluded-address

Command Purpose

To specify a single IP address or a range of IP addresses which the DHCP Server is not assign to DHCP clients, use the excluded-address DHCP pool configuration command. To remove the IP addresses, use the no form of this command.

Command Syntax

dhcp excluded-address *A.B.C.D* [*A.B.C.D*]

no dhcp excluded-address *A.B.C.D* [*A.B.C.D*]

Parameter	Parameter Description	Parameter Value
A.B.C.D	The excluded IP address, or low IP address in an excluded address range.	IPv4 Address
A.B.C.D(Optional)	The high IP address in the excluded address range.	IPv4 Address

Command Mode

Global Configuration

Default

All IP pool addresses are assignable.

Usage

The DHCP server assumes that all pool addresses may be assigned to clients. Use this command to exclude a single IP address or a range of IP addresses.

Examples

The following example shows how to disallow DHCP server distribute the address in the range of 10.10.1.100 -10.10.1.199:

```
Switch# configure terminal
Switch(config)# dhcp pool test
Switch(config-dhcp)# ip dhcp excluded-address 10.10.1.100 10.10.1.199
```

Related Commands

dhcp pool

4.4.19 show dhcp server conflict

Command Purpose

To display address conflicts found by a DHCP Server when addresses are offered to the client, use the show dhcp server conflict in privileged EXEC mode.

Command Syntax

show dhcp server conflict [ip A.B.C.D | all]

Parameter	Parameter Description	Parameter Value
ip A.B.C.D	Specifies the IP address of the conflict found.	IPv4 Address
all	Specifies all IP address of the conflict found.	-

Command Mode

Privileged EXEC

Default

None

Usage

The server detects conflicts using ping. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If an address conflict is detected, the address is removed from the pool and the address will not be assigned until an administrator resolves the conflict.

Examples

The following example displays the detection method and detection time for all IP addresses the DHCP server has offered that have conflicts with other devices:

```
Switch# show ip dhcp conflict all
```


Related Commands

clear dhcp server conflict
dhcp ping packets
dhcp ping timeout

4.4.20 show dhcp server binding

Command Purpose

To display address bindings on a DHCP Server, use the show dhcp server binding in privileged EXEC command.

Command Syntax

show dhcp server binding [ip *A.B.C.D* | pool *WORD* | all]

Parameter	Parameter Description	Parameter Value
ip A.B.C.D	Specifies the IP address of the conflict found.	IPv4 Address
pool WORD	Specifies the pool name where the IP address of the conflict found.	String with up to 31 characters
	Specifies all conflict IP address.	-

Command Mode

Privileged EXEC

Default

None

Usage

The binding address parameters including an IP address, an associated MAC address, a lease expiration date, and the type of address assignment that have occurred.

Examples

The following examples show the DHCP binding address parameters:

```
Switch# show ip dhcp binding 1.1.1.1
```

Related Commands

clear dhcp server binding

4.4.21 show dhcp server statistics

Command Purpose

To display DHCP Server statistics, use the show dhcp server statistics in privileged EXEC command.

Command Syntax

```
show dhcp server statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following example displays DHCP server statistics:

```
Switch#show dhcp server statistics
```

DHCP server packet statistics:

```
=====
```

Message Received

BOOTREQUEST	12
DHCPDISCOVER	200
DHCPREQUEST	178
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0

Message Sent

BOOTREPLY	12
DHCPOFFER	190
DHCPACK	172
DHCPNAK	6

Related Commands

clear dhcp server statistics

4.4.22 show dhcp server config

Command Purpose

To display the DHCP server configurations, use the show dhcp server config privileged EXEC command .

Command Syntax

show dhcp server config

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCP server.

Examples

The following is sample output from the show dhcp server config command:

```
Switch# show dhcp server config
```

```
DHCP server configuration:
```

```
=====
```

```
Pool name: pool10
```

```
network 10.1.1.0 mask 255.255.255.0
```

```
gateway 10.1.1.1
```

Related Commands

N/A

4.4.23 clear dhcp server conflict

Command Purpose

To clear an address conflict from the DHCP server database, use the clear dhcp server conflict privileged EXEC command.

Command Syntax

clear dhcp server conflict [ip A.B.C.D | all]

Parameter	Parameter Description	Parameter Value
ip A.B.C.D	The IP address of the host that contains the conflicting address you want to clear.	IPv4 Address
all	Clear all conflicting address.	-

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following example shows an address conflict of 1.1.1.99 being deleted from the DHCP server database:

```
Switch# clear ip dhcp conflict 1.1.1.99
```

Related Commands

show dhcp server conflict

4.4.24 clear dhcp server binding

Command Purpose

To delete an automatic address binding from the DHCP Server database, use the clear dhcp server binding in privileged EXEC command.

Command Syntax

clear dhcp server binding [ip *A.B.C.D* | pool *WORD* | all]

Parameter	Parameter Description	Parameter Value
ip A.B.C.D	The address of the binding you want to clear.	IPv4 Address
pool WORD	Specifies the pool name where the IP address of the conflict found.	String with up to 31 characters
all	Clears all automatic bindings.	-

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following example deletes the address binding 1.1.1.99 from a DHCP server database:

```
Switch# clear ip dhcp binding 1.1.1.99
```

Related Commands

show dhcp server binding

4.4.25 clear dhcp server statistics

Command Purpose

To reset all DHCP server counters, use the clear dhcp server statistics privileged EXEC command.

Command Syntax

clear dhcp server statistics

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following example resets all DHCP counters to zero:

```
Switch# clear dhcp server statistics
```

Related Commands

clear dhcp server statistics

4.4.26 show dhcp server pool**Command Purpose**

To display utilization of pool resources, use the show dhcp server pool in privileged EXEC mode.

Command Syntax

show dhcp server pool (*WORD* |)

Parameter	Parameter Description	Parameter Value
WORD	Specifies the pool name to display pool utilization.	String with up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following example shows resource utilization of a dhcp pool.:

```
Switch# show dhcp server pool pool1
```

```
Pool                : pool1
Type                : Dynamic
Lease               : 0 Days 0 Hours 5 Minutes
Total addresses     : 254
Leased addresses    : 1
Excluded addresses  : 1
Free addresses      : 252
Conflict addresses  : 0
Current index       IP address range      Leased/Excluded/Total
2.1.1.5             2.1.1.1 - 2.1.1.254      1 /1 /254
=====
```

Related Commands

4.5 DNS Commands

4.5.1 ip host

Command Purpose

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the `ip host` command in global configuration mode. If the hostname cache does not exist yet, it is automatically created.

To remove a hostname-to-address mapping, use the `no` form of this command.

Command Syntax

```
ip host HOSTNAME IP_ADDR
```

```
no ip host hostname
```

Parameter	Parameter Description	Parameter Value
HOSTNAME	Name of the host	String with up to 63 characters
IP_ADDR	Associated host IP address	IPv4 Address

Command Mode

Global Configuration

Default

No static hostname-to-address mapping is added to the DNS hostname cache for a DNS view.

Usage

None

Examples

The following example shows how to add a mapping entry to the global hostname cache and then remove one of those entries from the global hostname cache:

```
Switch# configure terminal
Switch(config)# ip host www.example1.com 192.0.2.141
```

Related Commands

show ip host

4.5.2 dns domain

Command Purpose

To specify the default domain for a Domain Name System (DNS) view to use to complete unqualified hostnames (names without a dotted-decimal domain name), use the `dns domain` command in global configuration mode.

To remove the specification of the default domain name for a DNS view, use the `no` form of this command.

Command Syntax

`dns domain DOMAIN-NAME`

`no dns domain DOMAIN-NAME`

Parameter	Parameter Description	Parameter Value
DOMAIN-NAME	Name of the domain	String with up to 63 characters

Command Mode

Global Configuration

Default

No default domain name is defined for the DNS view.

Usage

None

Examples

The following example shows how to specify the default domain for DNS:

```
Switch# configure terminal
Switch(config)# dns domain www.example1.com
```

Related Commands

show dns domain

4.5.3 dns server

Command Purpose

To add a name server to the list of Domain Name System (DNS) name servers, use the `dns server` command in global configuration mode. To remove a DNS name server from the list, use the `no` form of this command.

Command Syntax

`dns server IP_ADDR ( source-interface IFNAME | source-ip A.B.C.D | )`

`no dns server IP_ADDR`

Parameter	Parameter Description	Parameter Value
IP_ADDR	IP address of a DNS name server	Support IPv4/IPv6 Address
IFNAME	Name of source interface	Support physical/aggregation/loopback/tunnel/vlan ports
A.B.C.D	Source IP address	IPv4 Address

Command Mode

Global Configuration

Default

No IP address is explicitly added to the list of resolving name servers for this view.

Usage

This command can be entered multiple times to specify a maximum of three resolving name servers. After three resolving name servers have been specified, additional resolving name servers cannot be specified unless an existing entry is removed.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

The following example shows how to specify the DNS server list:

```
Switch# configure terminal
Switch(config)# dns server 10.10.1.1
Switch(config)# dns server 20.20.2.2
```

Related Commands

show dns server

4.5.4 show dns

Command Purpose

To display configuration information about a Domain Name System (DNS) view, use the show dns command in privileged EXEC mode.

Command Syntax

show dns { domain | server }

Parameter	Parameter Description	Parameter Value
domain	Display DNS domain list	-
server	Display DNS server list	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show dns domain command:

```
Switch# show dns domain
```

Current DNS domain configuration:

	Domain	Suffix
1	domain	domain.com
2	domain	aa.com

Related Commands

dns server

dns domain

4.5.5 show ip host

Command Purpose

To display configuration information about an ip host view, use the show ip host command in privileged EXEC mode.

Command Syntax

```
show ip host
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip host command:

```
Switch# show ip host
```

Current IP host configuration:

Host	Address

1	www.sampledomain.com	1.1.1.1

Related Commands

ip host

Chapter 5 IPv6 Service Commands

5.1 Tunnel Commands

5.1.1 interface

Command Purpose

Use this command to create a new tunnel interface.
Use the no form of this command to destroy the tunnel interface.

Parameter	Parameter Description	Parameter Value
TUNNEL-ID	The tunnel id	0-1023

Command Syntax

```
interface tunnel TUNNEL-ID  
no interface tunnel TUNNEL-ID
```

Command Mode

Global Configuration

Default

None

Usage

Before connect 2 IPv6 networks by an IPv4 network, a tunnel interface is required. The tunnel is available after set some attributes. After IPv6 is enabled the tunnel interface can forward IPv6 packets.

Examples

This example shows how to create a tunnel interface:

```
Switch# configure terminal  
Switch(config)# interface tunnel 1
```

Related Commands

show interface tunnel

5.1.2 tunnel mode

Command Purpose

Use this command to specify the IPv6 transition tunnel protocol.
Use the no form of this command to unset the tunnel protocol.

Command Syntax

```
tunnel mode tunnel mode ( erspan ( ecmp-dst-gre | ) | gre | ipv6ip ) ( 6to4 | isatap | )  
no tunnel mode
```

Parameter	Parameter Description	Parameter Value
6to4	Set the tunnel as automatic tunnel 6to4, which use 2002::/16 as its prefix	-
isatap	Set the tunnel as automatic tunnel ISATAP, which use ::5efe:a.b.c.d as its suffix	-
gre	When the destination of tunnel is single, the mode of the tunnel	-
ecmp-dst-gre	When the destinations of tunnel are multi, the mode of the tunnel	-

Command Mode

Interface Configuration

Default

None

Usage

This command specifies a tunnel encapsulation mode for IPv6 in IPv4. When the keywords "6to4" or "isatap" is not specified, then it is a manual tunnel. Tunnel mode is not allowed to change from 6to4 to ISATAP when 6to4 relay routes are configured. Users should unset the tunnel destination before change from manual tunnel to automatic tunnel.

Examples

This example shows how to create a 6to4 Tunnel:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel mode ipv6ip 6to4
```

Related Commands

tunnel source

tunnel destination

5.1.3 tunnel source**Command Purpose**

Use this command to specify the tunnel source. Use the no form of this command to unset the tunnel source.

Command Syntax

tunnel source (IP_ADDR | IFNAME)

no tunnel source

Parameter	Parameter Description	Parameter Value
IP_ADDR	Specify a tunnel source in the IPv4 address format	IPv4 Address
IFNAME	Specify a tunnel source in the IFNAME format, the IFNAME should be layer3 interface	Support physical/aggregation/loopback/vlan/ ports

Command Mode

Interface Configuration

Default

None

Every tunnel must have a tunnel source. If users specify the IFNAME format, system will choose the primary address as tunnel source.

Examples

This example shows how to set the tunnel source:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel source 3.3.3.3
```

Related Commands

tunnel mode ipv6ip

tunnel destination

5.1.4 tunnel destination

Command Purpose

Use this command to specify a tunnel destination address in an IPv4 portion.
Use the no parameter to un-specify the address.

Command Syntax

tunnel destination IP_ADDR
no tunnel destination

Parameter	Parameter Description	Parameter Value
IP_ADDR	Specify the tunnel destination IPv4 address	IPv4 Address

Command Mode

Interface Configuration

Default

None

Usage

Automatic tunnel such as 6to4 and ISATAP must not configure tunnel destination.

Examples

This example shows how to set the tunnel destination:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel destination 4.4.4.4
```

Related Commands

tunnel source
tunnel mode ipv6ip

Parameter	Parameter Description	Parameter Value
enable	Enable tunnel decapsulation	-
disable	Disable tunnel decapsulation	-

5.1.5 tunnel enable

Command Purpose

Use this command to enable tunnel decapsulation for interfaces. Use the form of this command to restore the default configuration.

Command Syntax

tunnel (enable | disable)

Command Mode

Interface Configuration

Default

By default, tunnel decapsulation is disabled on all interfaces.

Usage

None

Examples

This example shows how to enable tunnel decapsulation on interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# tunnel enable
```

Related Commands

Interface

5.1.6 tunnel ecmp-destination**Command Purpose**

Use this command to configure tunnel ECMP destinations IP address.
Use the form of this command to unset this configuration.

Command Syntax

```
tunnel ecmp-destination IP_ADDR
no tunnel ecmp-destination IP_ADDR
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	ECMP destinations IP address	IPv4 Address

Command Mode

Interface Configuration

Default

None

Usage

Automatic tunnel such as 6to4 and ISATAP must not configure tunnel destination (multi destination).

Examples

This example shows how to enable tunnel decapsulation on interface tunnel 1:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel ecmp-destination 1.1.1.1
Switch(config-if)# tunnel ecmp-destination 2.2.2.2
```

Related Commands

```
tunnel source
tunnel mode (ecmp-dst-gre | ) | gre
```


5.1.7 tunnel gre key

Command Purpose

Use this command to configure the tunnel gre key value.
Use the form of this command to unset this configuration

Command Syntax

tunnel gre key KEY_VALUE
no tunnel gre key

Parameter	Parameter Description	Parameter Value
KEY_VALUE	gre key value	1-4294967295

Command Mode

Interface Configuration

Default

None

Usage

Improve the security of the gre tunnel, configure the gre key to do the checkout of point to point.

Examples

This example shows how to enable tunnel decapsulation on interface tunnel 1:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel gre key 100
```

Related Commands

show running-config interface tunnel

5.1.8 tunnel extend-header

Command Purpose

Before the mirror traffic passes through the tunnel, encapsulate the traffic with the extend header.
Use no the form of this command to unset this configuration.

Command Syntax

tunnel extend-header
no tunnel extend-header

Command Mode

Interface Configuration

Default

None

Usage

- spanExtendHeaderCopyHash, using the new hash or not;
- PacketInfo.skipTimeInfoUpdate, fixed with 1;

- if spanExtendHeaderCopyHash is 1, the field consists with hash (8 bit) and 0 (8 bit); if spanExtendHeaderCopyHash is 0, the field consists with source port of the mirror (16 bit).

Without dst-load-balance parameter, spanExtendHeaderCopyHash will be 0, and extend-header field does not contain the hash value; with dst-load-balance parameter, spanExtendHeaderCopyHash will be 1, and extend-header field contains the hash value.

Examples

This example shows how to enable extend-header hash for load balance:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel extend-header
```

```
Switch(config-if)# tunnel extend-header dst-load-balance
```

Related Commands

```
show running-config interface tunnel
```

5.1.9 tunnel extend-header id

Command Purpose

Use this command to configure the extend header id.
Use the no form of this command to unset this configuration.

Command Syntax

```
tunnel extend-header id ID_VALUE
```

```
No tunnel extend-header id ID_VALUE
```

Parameter	Parameter Description	Parameter Value
ID_VALUE	The extend header id value	1-1023

Command Mode

Interface Configuration

Default

0

Usage

None

Examples

This example shows how to enable tunnel decapsulation on interface tunnel 1:

```
Switch# configure terminal
```

```
Switch(config)# interface tunnel 1
```

```
Switch(config-if)# tunnel extend-header id 30
```

Related Commands

```
show running-config interface tunnel
```

5.1.10 tunnel dscp

Command Purpose

Use this command to specify a value of Differentiated Services Code Point (DSCP) in the tunnel IPv4 encapsulation header.
Use the no parameter to inherit the underlying physical interface value by default.

Command Syntax

tunnel dscp DSCP
no tunnel dscp

Parameter	Parameter Description	Parameter Value
DSCP	The outer IPv4 header DSCP value	0-63

Command Mode

Interface Configuration

Default

By default, the DSCP value is inherited from original IPv6 packet.

Usage

None

Examples

This example shows how to set the outer IPv4 header DSCP value as 40:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel dscp 40
```

Related Commands

Interface

5.1.11 tunnel ttl**Command Purpose**

Use this command to specify a value of time to live (TTL) in the tunnel IPv4 encapsulation header.
Use the no parameter to inheriting the underlying physical interface value by default.

Command Syntax

tunnel ttl TTL
no tunnel TTL

Parameter	Parameter Description	Parameter Value
TTL	The outer IPv4 header TTL value	1-254

Command Mode

Interface Configuration

Default

By default, the TTL value is inherited from original IPv6 packet.

Usage

None

Examples

This example shows how to set the outer IPv4 header TTL value as 254:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# tunnel ttl 254
```

Related Commands

Interface

5.1.12 ipv6 mtu

Command Purpose

Use this command to specify the Tunnel interface MTU.
Use the no form of this command to restore to the default value.

Command Syntax

```
ipv6 mtu MTU
no ipv6 mtu
```

Parameter	Parameter Description	Parameter Value
MTU	Set the tunnel interface MTU	1280-9500

Command Mode

Interface Configuration

Default

1480

Usage

System does not support Path MTU Discovery on tunnel interface. This command is only allowed on tunnel interface.

Examples

This example sets the tunnel interface MTU to 1280:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ipv6 mtu 1280
```

Related Commands

tunnel ttl

5.1.13 show interface tunnel

Command Purpose

Use this command to display the tunnel information.

Command Syntax

```
show interface tunnel TUNNEL-ID
```

Parameter	Parameter Description	Parameter Value
TUNNEL-ID	The tunnel id	0-1023

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays the tunnel information:
Switch# show interface tunnel1

```
Interface tunnel1
Interface current state: UP
Hardware is Tunnel
Index 8193 , Metric 1 , Encapsulation TUNNEL
VF binding: not bound
Tunnel protocol/transport IPv6/IP, Status Valid
Tunnel source 1.1.1.1(eth-0-1), destination 2.2.2.2
Tunnel DSCP inherit, Tunnel TTL 64
Tunnel transport MTU 1480 bytes
```

Related Commands

show ipv6 interface tunnel

5.1.14 show resource tunnel**Command Purpose**

Use this command to display the tunnel peers resource information.

Command Syntax

show resource tunnel

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays the tunnel peers resource information:

```
Switch# show resource tunnel
```

```
Tunnel
```

```
Resource                Used          Capability
```

```
=====
```

```
Peers                   1          8
```

Related Commands

None

5.2 NDP Commands

5.2.1 ipv6 neighbor

Command Purpose

Use this command to configure a static neighbor entry.
To delete the static neighbor entry, use the no form of this command.

Command Syntax

```
ipv6 neighbor ( vrf NAME | ) IPV6_ADDR MAC ( IFNAME | )
```

```
no ipv6 neighbor ( vrf NAME | ) IPV6_ADDR ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
vrf NAME	vrf instance name	String with up to 15 characters
IPV6_ADDR	IPv6 address in X:X::X:X format	IPv6 Address
MAC	MAC address in HHHH.HHHH.HHHH format	MAC Address
IFNAME	Interface name	Support physical/aggregation/loop back/vlan/tunnel ports

Command Mode

Global Configuration

Default

By default, there is not any static ipv6 neighbor entry exist.

Usage

Use this command to configure a static neighbor entry. If the IPv6 address is link-local, the interface name must be specified.
Using the no form of this command should not remove any dynamic neighbor entries.

Examples

This example shows how to add a static neighbor entry:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 neighbor 2001::1 0000.0000.0001
```

```
Switch(config)# ipv6 neighbor vrf a fe80::1 0000.0000.0002 eth-0-1
```

Related Commands

show ipv6 neighbors

5.2.2 clear ipv6 neighbors

Command Purpose

Use this command to clear the dynamic neighbor entries.

Command Syntax

clear ipv6 neighbors (vrf *NAME* |) (interface *IFNAME* |)

Clearipv6 neighbors (vrf *NAME* |) *IPv6_ADDR* (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
vrf NAME	vrf instance name	String with up to 15 characters
interface IFNAME	Clear neighbor cache on the interface	Supportphysical/aggregation/loop back/vlan/tunnel ports
IPv6_ADDR	IPv6 address in X:X::X:X format. Clear IPv6 neighbor cache by address	IPv6 Address

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to clear the dynamic neighbor entries.

User can clear dynamic ipv6 address by interface or address. If the specified address is link-local, the interface is required.

Examples

This example shows how to clear the neighbor entries:

```
Switch# clear ipv6 neighbors
```

Related Commands

show ipv6 neighbors

5.2.3 ipv6 hop-limit

Command Purpose

Use this command to set the ipv6 hop limit of the packets.

To restore the default configuration, use the no form of this command.

Command Syntax

ipv6 hop-limit *HOP_LIMIT*

no ipv6 hop-limit

Parameter	Parameter Description	Parameter Value
hop-limit HOP_LIMIT	Hop limit.	1-255

Command Mode

Global Configuration

Default

By default, the value is 64.

Usage

The hop limit setting should affect all IPv6 packets send from this device, unless the hop-limit is overwritten by up layer application, for example, OSPF, etc.

Examples

This example shows how to set the hop limit:

```
Switch# configure terminal
Switch(config)# ipv6 hop-limit 255
```

Related Commands

None

5.2.4 ipv6 nd ra hop-limit

Command Purpose

Use this command to set the "Current hop limit" in RA packets.
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd ra hop-limit HOP_LIMIT
no ipv6 nd ra hop-limit
```

Parameter	Parameter Description	Parameter Value
hop-limit HOP_LIMIT	Set cur hop limit.	0-255

Command Mode

Interface Configuration

Default

By default, the value is 0.

Usage

None

Examples

This example shows how to set the "Current hop limit" in RA packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra hop-limit 255
```

Related Commands

None

5.2.5 ipv6 nd dad attempts

Command Purpose

Use this command to set the attempt times of DAD (Duplicate Address Detect).
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd dad attempts DAD_ATTEMPTS  
no ipv6 nd dad attempts
```

Command Mode

Parameter	Parameter Description	Parameter Value
DAD_ATTEMPTS	Set attempts number.	0-600

Interface Configuration

Default

By default, the value is 1.

Usage

Use this command to set the attempt times of DAD (Duplicate Address Detect). "0" means DAD feature is disabled

Examples

This example shows how to set the dad attempt:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# ipv6 nd dad attempts 3
```

Related Commands

None

5.2.6 ipv6 nd ns-interval

Command Purpose

Use this command to set the interval of NS packets.
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd ns-interval NS_INTERVAL  
no ipv6 nd ns-interval
```

Command Mode

Interface Configuration

Parameter	Parameter Description	Parameter Value
NS_INTERVAL	Set IPv6 neighbor solicitation interval.	1000-3600000 milliseconds

Default

By default, the value is 1000

Usage

This configuration should affect the interval of NS packet during the DAD period or neighbor discovery period.

Example

This example shows how to set the ns interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ns-interval 2000
```

Related Commands

None

5.2.7 ipv6 nd ra suppress

Command Purpose

Use this command to enable the RA suppress function.
To disable this function, use the no form of this command.

Command Syntax

```
ipv6 nd ra suppress
no ipv6 nd ra suppress
```

Command Mode

Interface Configuration

Default

By default, RA suppress is enabled.

Usage

When RA suppress function is enabled, no RA/RS packet should be sent from this interface even a RS packet is received.

Examples

This example shows how to enable the RA suppress function:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra suppress
```

This example shows how to disable the RA suppress function:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 nd ra suppress
```

Related Commands

```
ipv6 nd ra interval
ipv6 nd ra lifetime
```

5.2.8 ipv6 nd ra mtu suppress

Command Purpose

Use this command to enable the RA MTU suppress function.
To disable this function, use the no form of this command.

Command Syntax

```
ipv6 nd ra mtu suppress
no ipv6 nd ra mtu suppress
```

Command Mode

Interface Configuration

Default

By default, RA MTU suppress is disabled.

Usage

When RA MTU suppress function is enabled, no MTU option should be sent in the RA packets from this interface.

Examples

This example shows how to enable the RA MTU suppress function:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra mtu suppress
```

This example shows how to disable the RA MTU suppress function:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 nd ra mtu suppress
```

Related Commands

None

5.2.9 ipv6 nd ra interval

Command Purpose

Use this command to set the interval of the RA packets.
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd ra interval MAX ( MIN | )
no ipv6 nd ra interval
```

Command Mode

Interface Configuration

Parameter	Parameter Description	Parameter Value
MAX	RA max interval (sec).	4-1800 seconds
MIN	RA min interval (sec).	3-1350 seconds

Default

By default, MAX interval should be 600 second; MIN interval should be $0.33 \times \text{MAX}$.

Usage

The valid range should be between 4 and 1800 second for the max value. The valid range should be between 3 and $0.75 \times \text{MAX}$ for the minimum value.

If the minimum value is not specified, it should be $0.33 \times \text{MAX}$ when $\text{MAX} \geq 9$, and it should be equal to the MAX when $\text{MAX} < 9$.

Examples

This example shows how to set the RA interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra interval 300
```

Related Commands

```
ipv6 nd ra suppress
ipv6 nd ra lifetime
```

5.2.10 ipv6 nd ra lifetime

Command Purpose

Use this command to set the life time of the RA packets.
To restore the default configuration, use the no form of this command.

Command Syntax

```
ipv6 nd ra lifetime LIFE_TIME
no ipv6 nd ra lifetime
```

Parameter	Parameter Description	Parameter Value
LIFE_TIME	Set IPv6 router advertisement lifetime.	0-9000 seconds

Command Mode

Interface Configuration

Default

By default, RA life time is 3* MAX RA interval.

Usage

None

Examples

This example shows how to set the ra life time:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd ra lifetime 1000
```

Related Commands

```
ipv6 nd ra suppress
ipv6 nd ra interval
```

5.2.11 ipv6 nd reachable-time

Command Purpose

Use this command to set reachable time of the neighbor entries.
To restore the default configuration, use the no form of this command

Command Syntax

Parameter	Parameter Description	Parameter Value
REACHABLE_TIME	Reachability time in milliseconds.	0-3600000 milliseconds

```
ipv6 nd
```

```
reachable-time REACHABLE_TIME
no ipv6 nd reachable-time
```

Command Mode

Interface Configuration

Default

By default, the value is 30000 ms

Usage

A reachable time 0 means to restore the default value 30000.

After the reachable time expired, the neighbor entries which state is "REACH" should change to "STALE".

Examples

This example shows how to set the reachable time:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd reachable-time 3600000
```

Related Commands

None

5.2.12 ipv6 nd managed-config-flag

Command Purpose

Use this command to set "Managed address configuration" flag.
To unset this configuration, use the no form of this command.

Command Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Command Mode

Interface Configuration

Default

By default, the "Managed address configuration" is not set.

Usage

None

Examples

This example shows how to set the "Managed address configuration" flag:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd managed-config-flag
```

Related Commands

ipv6 nd other-config-flag

5.2.13 ipv6 nd other-config-flag

Command Purpose

Use this command to set the "Other configuration" flag.
To unset this configuration, use the no form of this command.

Command Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Command Mode

Interface Configuration

Default

By default, the "Other configuration" flag is not set.

Usage

None

Examples

This example shows how to set the "Other configuration" flag:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd other-config-flag
```

Related Commands

ipv6 nd managed-config-flag

5.2.14 ipv6 nd prefix

Command Purpose

Use this command to set prefix for route advertise (RA).
To unset a prefix to advertise, use the no form of this command.

Command Syntax

```
ipv6 nd prefix IPv6_PREFIX ( VALID_TIME | infinite ) ( PREFERRED_TIME | infinite ) ( { off-link | no-autoconfig } | )
no ipv6 nd prefix IPv6_PREFIX
ipv6 nd prefix default ( VALID_TIME | infinite ) ( PREFERRED_TIME | infinite ) ( { off-link | no-autoconfig } | )
no ipv6 nd prefix default
```

Parameter	Parameter Description	Parameter Value
IPv6_PREFIX	Configure IPv6 routing prefix advertisement. IPv6 prefix in X::X::X/M format	IPv6 Address and mask length
VALID_TIME	Valid lifetime.	0-4294967295 second
PREFERRED_TIME	Preferred lifetime.	0-4294967295 second

Command Mode

Interface Configuration

Default

The valid range of valid life time should be between 0 and 4294967295 seconds. User can also use the keyword "infinite" to indicate the value 4294967295(0xFFFFFFFF) . The default value should be 2592000 seconds (30 days).
The valid range of preferred life time should be between 0 and 4294967295 seconds. User can also use the keyword "infinite" to indicate the value 4294967295 (0xFFFFFFFF) . The default value should be 604800 seconds (7 days).

Usage

None

Examples

This example shows how to set the prefix:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 nd prefix 2001::1/64 3000 3000
```

Related Commands

show ipv6 interface IFNAME prefix

5.2.15 show ipv6 interface IFNAME prefix

Command Purpose

Use this command to show the prefix for route advertise (RA) on the specified interface.

Command Syntax

show ipv6 interface *IFNAME* prefix

Command Mode

Parameter	Parameter Description	Parameter Value
IFNAME	Name of the interface to show	Support physical/aggregation/loopback/vlan/tunnel ports

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the result of this command:

```
Switch# show ipv6 interface eth-0-1 prefix
```

Related Commands

ipv6 nd prefix

5.2.16 show ipv6 neighbors

Command Purpose

Use this command to show all ipv6 neighbor entries.

Command Syntax

show ipv6 neighbors (dynamic | static | interface *IFNAME* | *IPv6_ADDR* | statistics |)

Parameter	Parameter Description	Parameter Value
interface IFNAME	Name of the interface to show	Support physical/aggregation/loopback/vlan/tunnel ports
IPv6_ADDR	IPv6 address in X:X::X:X format	IPv6 Address

Command Mode

Privileged EXEC

Default

None

Usage

Neighbor entries should be able to show globally, by interface, or by prefix. Dynamic and static entries can be displayed separately.

Examples

This example shows the result of this command:

```
Switch# show ipv6 neighbors
```

IPv6 address	Age	Link-Layer Addr	State	Interface
2001::2	7	40f2.fd60.ac00	REACH	eth-0-9
fe80::42f2:fdff:fe60:ac00	6	40f2.fd60.ac00	STALE	eth-0-9

Related Commands

ipv6 neighbor

5.2.17 debug ipv6 nd

Command Purpose

Use this command to open the debug of ipv6 ND feature.

To close the debug of ipv6 ND feature, use the no form of this command.

Command Syntax

debug ipv6 nd (packet | events | error | dump | info | all)

no debug ipv6 nd (packet | events | error | dump | info | all)

Parameter	Parameter Description	Parameter Value
packet	IPv6 ND packet	-
events	IPv6 ND events	-
error	IPv6 ND Error message	-
dump	Dump message in hex format	-
info	IPv6 ND information	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

By default, the ipv6 nd debug is closed.

Usage

None

Examples

This example shows how to open the ipv6 ND debug:

```
Switch# debug ipv6 nd all
```

```
Switch# terminal monitor
```

Related Commands

None

5.3 DHCPv6 Relay Commands

5.3.1 dhcpv6 relay

Command Purpose

To enable the DHCPv6 relay service, use the `dhcpv6 relay` command in global configuration mode.
To disable this function, use the `no` form of this command.

Command Syntax

```
dhcpv6 relay
no dhcpv6 relay
```

Command Mode

Global Configuration

Default

DHCPv6 relay is disabled.

Usage

The DHCPv6 service must be enabled with the `dhcpv6 service` command before DHCPv6 relay service can be used.

Examples

The following example shows how to enable DHCPv6 relay agent:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay
```

Related Commands

```
service dhcpv6
```

5.3.2 dhcpv6-server (global)

Command Purpose

To create a DHCPv6 server group, use the `dhcpv6-server` command in global configuration mode.
To remove a DHCPv6 server group, use the `no` form of this command.

Command Syntax

```
dhcpv6-server NUMBER IPV6_ADDR interface IFNAME
no dhcpv6-server NUMBER ( IPV6_ADDR ( interface IFNAME | ) )
```

Parameter	Parameter Description	Parameter Value
NUMBER	Number of the DHCPv6 server group. The range is from 1 to 16	1-16
IPV6_ADDR	The IPv6 address list of the DHCPv6 server. The range in number of the servers in a list is 1 to 8	IPv6 address
IFNAME	The name of supported interface	Supportphysical/aggregation/vlan ports

Command Mode

Global Configuration

Default

No DHCPv6 server group is defined.

Usage

This command is used to specify the remote DHCPv6 server .

Examples

The following example shows how to configure dhcpv6-server group globally:

```
Switch# configure terminal
Switch(config)# dhcpv6-server 1 2001:1::1
Switch(config)# dhcpv6-server 1 fe80::1 interface vlan1
```

Related Commands

service dhcpv6
dhcpv6-server (interface)

5.3.3 dhcpv6-server (interface)

Command Purpose

To add an interface into a DHCPv6 server group, use the dhcpv6-server command in interface configuration mode. To remove this interface from the DHCPv6 server group, use the no form of this command.

Command Syntax

dhcpv6-server *NUMBER*
no dhcpv6-server

Command Mode

Parameter	Parameter Description	Parameter Value
NUMBER	Number of the DHCPv6 server group.	1-16

Interface Configuration

Default

No DHCPv6 server group is configured for the interface.

Usage

This command is used to specify DHCPv6 server group which is configured by the command dhcpv6-server in global mode.

Examples

The following example shows how to configure dhcpv6-server group for interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcpv6-server 1
```

Related Commands

service dhcpv6

5.3.4 dhcpv6 relay remote-id option

Command Purpose

To enable remote-id option, use the dhcpv6 relay remote-id option command in global configuration mode. To disable remote-id option, use the no form of this command.

Command Syntax

dhcpv6 relay remote-id option
no dhcpv6 relay remote-id option

Command Mode

Global Configuration

Default

Remote-id option is not added into DHCPv6 RELAY_FORW packet sent by relay.

Usage

None

Examples

The following example shows how to enable remote-id option:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay remote-id option
```

Related Commands

dhcpv6 relay remote-id format

5.3.5 dhcpv6 relay remote-id format

Command Purpose

To specify the format of remote-id , use the dhcpv6 relay remote-id format command in global configuration mode. To restore the default format, use the no form of this command.

Command Syntax

```
dhcpv6 relay remote-id format { vlan | ifname | duid }
no dhcpv6 relay remote-id format
```

Parameter	Parameter Description	Parameter Value
vlan	The ID of the vlan attached by client	
ifname	The name of the interface received packet from client	
duid	The duid of relay	

Command Mode

Global Configuration

Default

The remote-id format is "duid:ifname:".

Usage

The format of remote-id can be a combination of vlan, interface name, DUID. This command specifies the existing keywords in the combination.

Examples

The following example shows how to specify the format of remote-id:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay remote-id format vlan
```

Related Commands

dhcpv6 relay remote-id option

5.3.6 dhcpv6 relay pd route

Command Purpose

To enable learning route from prefix-delegation option, use the dhcpv6 relay pd route command in global configuration. To disable the function, use the no form of this command.

Command Syntax

```
dhcpv6 relay pd route
no dhcpv6 relay pd route
```

Command Mode

Global Configuration

Default

The DHCPv6 relay won't learn prefix-delegation route.

Usage

The DHCPv6 relay can learn route from prefix delegated by server to client. This kind of route should not replace static one. Use this command to enable this function.

Examples

The following example shows how to enable learning route from prefix-delegation option:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay pd route
```

Related Commands

```
clear dhcpv6 relay pd route
dhcpv6 relay pd route distance
```

5.3.7 dhcpv6 relay pd route distance

Command Purpose

To configure the default distance for route learned by relay, use the dhcpv6 relay pd route distance command in global configuration. To restore the default value, use the no form of this command..

Command Syntax

```
dhcpv6 relay pd route distance DISTANCE
no dhcpv6 relay pd route distance
```

Command Mode

Parameter	Parameter Description	Parameter Value
DISTANCE	The default distance for route learned by relay	1-255

Global Configuration

Default

The default value of distance is 254.

Usage

Use this command to configure the distance of the route learned by relay from prefix-delegation.

Examples

The following example shows how to configure the distance of route added by DHCPv6 relay:

```
Switch# configure terminal
Switch(config)# dhcpv6 relay pd route distance 233
```

Related Commands

dhcpv6 relay pd route

5.3.8 service dhcpv6

Command Purpose

To enable the Dynamic Host Configuration Protocol (DHCP)V6 relay agent features on your router, use the service dhcpv6 command in global configuration mode.

To disable the DHCPv6 relay agent features, use the no form of this command.

Command Syntax

```
service dhcpv6 enable
service dhcpv6 disable
```

Command Mode

Global Configuration

Default

DHCPv6 service is disabled globally.

Usage

Only the main DHCPv6 service is enabled by the service dhcpv6 command, other DHCPv6 services could be used, such as dhcpv6 relay.

Examples

The following example shows how to enable DHCPv6 service globally:

```
Switch# configure terminal
Switch(config)# service dhcpv6 enable
```

Related Commands

dhcpv6 relay

5.3.9 debug dhcpv6 relay

Command Purpose

Use this command to turn on the debug switches of DHCPv6 relay module.

To restore the default, use the no form of this command

Command Syntax

```
debug dhcpv6 relay ( events | error | dump | packet | all )
no debug dhcpv6 relay ( events | error | dump | packet | all )
```

Parameter	Parameter Description	Parameter Value
events	Relay events	-
error	Error DHCP message	-
packet	DHCP message fields	-
dump	Dump message in hex format	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.
Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcpv6 relay debug switches:
Switch# debug dhcpv6 relay all

Related Commands

terminal monitor
show logging buffer

5.3.10 show dhcpv6-server**Command Purpose**

To display the DHCPv6 server groups, use the show dhcpv6-server command in privileged EXEC mode.

Command Syntax

show dhcpv6-server

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display all the DHCPv6 server groups configured with command dhcpv6-server in global mode.

Examples

The following example shows how to display dhcpv6-server group information:
Switch# show dhcpv6-server

DHCPv6 server group information:

```
=====
group 1 ipv6 address list:
[1] 2001:1::1
```

Related Commands

dhcpv6-server (global)

5.3.11 show dhcpv6 relay interfaces**Command Purpose**

To display to which dhcpv6-server group the interface belongs, use the show dhcpv6 relay interfaces command in privileged EXEC mode.

Command Syntax

show dhcpv6 relay interfaces

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the interface which is confined DHCPv6 relay.

Examples

The following example shows how to display dhcpv6 relay interfaces information:

Switch# show dhcpv6 relay interfaces

List of DHCPv6 relay enabled interface(s):

DHCPv6 relay service status: enabled

Interface Name	DHCPv6 server group

eth-0-1	1

Related Commands

show dhcpv6-server

5.3.12 show dhcpv6 relay pd client**Command Purpose**

To display the result of DHCPv6 relay's prefix-delegation route function, use the show dhcpv6 relay pd client command in privileged EXEC mode.

Command Syntax

show dhcpv6 relay pd client

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display information of prefix-delegation route:

Switch# show dhcpv6 relay pd client

DHCPv6 prefix-delegation client information:

```
=====
Interface   : vlan2
Client DUID  : 0001000117e9357b606da182030
Client IPv6 address : fe80::626d:a1ff:fe82:300
IA ID       : a18230
IA Prefix   : 2002:2:10::/64
              preferred/max lifetime : 280/300
              expired time : 2012-09-17 11:43:59
=====
```

Related Commands

dhcpv6 relay pd route
dhcpv6 relay pd route distance

5.3.13 show dhcpv6 relay statistics**Command Purpose**

To display the statistics of DHCPv6 packets relayed by the switch, use the show dhcpv6 relay statistics command in privileged EXEC mode.

Command Syntax

show dhcpv6 relay statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display detail DHCPv6 statistics which processed by the switch.

Examples

The following example shows how to display DHCPv6 relay statistics:

```
Switch# show dhcpv6 relay statistics
```

```
DHCPv6 relay packet statistics:
```

```
=====
Client relayed packets:  48
Server relayed packets:  48
Client error packets:    0
Server error packets:    0
```

Related Commands

clear dhcpv6 relay statistics

5.3.14 clear dhcpv6 relay statistics**Command Purpose**

To reset the statistics of DHCPv6 packets relayed by the switch, use the clear dhcpv6 relay statistics command in privileged EXEC mode.

Command Syntax

clear dhcpv6 relay statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to reset DHCPv6 statistics.

Examples

The following example shows how to clear DHCPv6 relay statistics:


```
Switch# clear dhcpv6 relay statistics
```

Related Commands

show dhcpv6 relay statistics

5.3.15 clear dhcpv6 relay pd route

Command Purpose

To clear the route learned by DHCPv6 relay from prefix-delegation, use the clear dhcpv6 relay pd route command in privileged EXEC mode.

Command Syntax

```
clear dhcpv6 relay pd route ( prefix PREFIX | ) ( interface IFNAME | ) ( IPv6_ADDR | )
```

Parameter	Parameter Description	Parameter Value
PREFIX	The prefix delegated to client	IPv6 Address and mask length in X:X::X:X/M format
IPv6_ADDR	The IPv6 address of PD client	IPv6 Address
IFNAME	The name of supported interface	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

If no parameter is specified, all route will be cleared.

Examples

The following example shows how to clear route learned by DHCPv6 relay:

```
Switch# clear dhcpv6 relay pd route interface eth-0-1
```

Related Commands

dhcpv6 relay pd route

show dhcpv6 relay pd client

Chapter 6 IP Routing Commands

6.1 IP Unicast-Routing Commands

6.1.1 ip address

Command Purpose

To set a primary or secondary IP address for an interface, use the ip address command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.

Command Syntax

ip address (ADDRESS WILDCARD-MASK | ADDRESS /PREFIX-LENGTH) (secondary |)

Parameter	Parameter Description	Parameter Value
ADDRESS	IPv4 address of the interface	IPv4 address
WILDCARD-MASK	Mask for the associated IP subnet	Mask in IPv4 address format
PREFIX-LENGTH	Prefix length of the address	1-32
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address	-

Command Mode

Interface Configuration

Default

No IP address is defined for the interface.

Usage

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the switch always use the primary IP address. Therefore, all switches and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Switch respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the no ip address command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional secondary keyword allows you to specify up to 8 secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

There may not be enough host addresses for a particular network segment. For example, your subnet allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the switches or access servers allows you to have two logical subnets using one physical subnet.

Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnet and router-based network. Switches on an older, bridged segment can be easily made aware that many subnets are on that segment. Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is extended, or layered on top of the second network using secondary addresses.

Examples

In the following example, 10.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17/24 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
```

Related Commands

None

6.1.2 ip icmp error-interval

Command Purpose

To set the interval of ICMP error messages generated by the switch, use the `ip icmp error-interval` command in global configuration mode. To restore the default value, use the `no` form of this command.

Command Syntax

```
ip icmp error-interval INTERVAL
no ip icmp error-interval
```

Parameter	Parameter Description	Parameter Value
INTERVAL	The interval in milliseconds.	0 - 2147483647 milliseconds

Command Mode

Global Configuration

Default

Default is 1000 milliseconds.

Usage

None

Examples

In the following example, user sets the error interval to 10 seconds, which means only one ICMP error message was generated per 10 seconds:

```
Switch# configure terminal
Switch(config)# ip icmp error-interval 10000
```

Related Commands

ip redirects
ip unreachable

6.1.3 ip redirects

Command Purpose

To enable send the ICMP redirect messages generated by the switch, use the ip redirects command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

ip redirects
no ip redirects

Command Mode

Interface Configuration

Default

IP redirect is enabled by default.

Usage

None

Examples

In the following example, users disable to send the ICMP redirect message:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
```

```
Switch(config-if)# no ip redirects
```

Related Commands

ip unreachable
ip icmp error-interval

6.1.4 ip unreachable

Command Purpose

To enable send the ICMP unreachable messages generated by the switch, use the ip unreachable command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

ip unreachable
no ip unreachable

Command Mode

Interface Configuration

Default

IP unreachable is enabled by default.

Usage

None

Examples

In the following example, users disable to send the ICMP unreachable message:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config-if)# no ip unreachable
```

Related Commands

ip redirects
ip icmp error-interval

6.1.5 ip verify unicast reverse-path

Command Purpose

To enable RPF check to the interface, use the command `ip verify unicast reverse-path` in interface configuration mode. To restore the default value, use the `no` form of this command.

Command Syntax

```
ip verify unicast reverse-path
no ip verify unicast reverse-path
```

Command Mode

Interface Configuration

Default

RPF check is disabled by default.

Usage

None

Examples

In the following example, users enable RPF check in interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1/24
Switch(config)# ip verify unicast reverse-path
```

Related Commands

```
ip redirects
ip icmp error-interval
```

6.1.6 unicast reverse-path check-type (strict| loose (allow-default-route|))

Command Purpose

Use this command to configure RPF check type to the interface in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

```
unicast reverse-path check-type ( strict | loose ( allow-default-route | ) )  
no unicast reverse-path check-type
```

Command Mode

Interface Configuration

Default

RPF check-type is strict by default.

Usage

RPF check-type takes effect for both ipv4 and ipv6.

Examples

In the following example, users configure RPF check-type loose in interface eth-0/1:

```
Switch# configure terminal  
Switch(config)# interface eth-0/1  
Switch(config-if)# no switchport  
Switch(config)# unicast reverse-path check-type loose
```

Related Commands

None

6.1.7 router-id (global)

Command Purpose

To use a fixed router ID for all routing protocols, use the router-id command in global configuration mode. To let switch select the router ID automatically, use the no form of this command.

Command Syntax

```
router-id IP-ADDRESS
```

no router-id

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	Router ID in IP address format	IPv4 address

Command Mode

Global Configuration

Default

No router ID is defined.

Usage

You can configure an arbitrary value in the IP address format for each switch. However, each router ID must be unique.

Examples

The following example specifies a fixed router-id:

```
Switch# configure terminal
Switch(config)# router-id 1.1.1.1
```

Related Commands

router-id (router)

6.1.8 ip route

Command Purpose

To establish static routes, use the ip route command in global configuration mode. To remove static routes, use the no form of this command.

Command Syntax

ip route (*VRF NAME* |) (*PREFIX MASK* | *PREFIX/PREFIX-LENGTH*) (*NH-ADDRESS* | *IFNAME*) (*DISTANCE* |) (track *NUMBER* |)

Parameter	Parameter Description	Parameter Value
VRF NAME	VRF instance name	A string up to 16 characters
PREFIX	IP route prefix for the destination	IPv4 address
MASK	Prefix mask for the destination	Mask in IPv4 address format
PREFIX-LENGTH	Prefix length for the destination	1-32
NH-ADDRESS	IP address of the next hop that can be used to reach that network	IPv4 address

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name of the next hop that can be used to reach that network.	Only support tunnel and null interface
DISTANCE	(Optional) An administrative distance. The default administrative distance for a static route is 1	1-255
track NUMBER	Specify the ID of track object	1-500

Command Mode

Global Configuration

Default

No static routes are established.

Usage

The establishment of a static route is appropriate when the switch cannot dynamically build a route to the destination.

Examples

The following example establishes a static route:

```
Switch# configure terminal
Switch(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example establishes a static route which nexthop is blackhole:

```
Switch# configure terminal
Switch(config)# ip route 10.1.1.1/32 null 0
```

Related Commands

show ip route

6.1.9 show ip route

Command Purpose

To display the current state of the routing table, use the show ip route command in user EXEC or privileged EXEC mode.

Command Syntax

show ip route (*VRF NAME* |) (*IP-ADDRESS* | *PREFIX/PREFIX-LENGTH* | *PROTOCOL* |)

Parameter	Parameter Description	Parameter Value
VRF NAME	VRF instance name	A string up to 15 characters

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	(Optional) Address about which routing information should be displayed	IPv4 address
PREFIX	IP route prefix	IPv4 address
PREFIX-LENGTH	Prefix length for the route	1-32
PROTOCOL	(Optional) The name of a routing protocol, or the keyword connected, static, or summary. If you specify a routing protocol, use one of the following keywords: bgp, ospf, and rip.	bgp/connected/isis/ospf/rip/static

Command Mode

Privileged EXEC

Default

None

Usage

You can display all active dynamic and static routes with both the show ip route and show ip route static commands after these active routes are added in the main routing table.

Examples

The following is sample output from the show ip route command when entered without an address:

```
Switch# show ip route
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
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
```

```
[*] - [AD/Metric]
```

```
* - candidate default
```

```
O    1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:34:17
```

```
O    2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
```

```
C    10.10.1.0/24 is directly connected, eth-0-23
```

```
C    10.10.1.23/32 is in local loopback, eth-0-23
```

```
O    10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:17:26
```

```
O    10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:17:26
```

Related Commands

ip route

show ip route database

6.1.10 show ip route database

Command Purpose

To display the Routing Information Base (RIB), use the show ip route database command in user EXEC or privileged EXEC mode.

Command Syntax

show ip route database (*VRF NAME* |) (*PROTOCOL* |)

Parameter	Parameter Description	Parameter Value
VRF NAME	VRF instance name	A string up to 15 characters
PROTOCOL	(Optional) The name of a routing protocol, or the keyword connected, static, or summary. If you specify a routing protocol, use one of the following keywords: bgp, ospf, and rip.	bgp/connected/isis/ospf/rip/static

Command Mode

Privileged EXEC

Default

None

Usage

You can display all active dynamic and static routes with both the show ip route database and show ip route database static commands after these active routes are added in the Routing Information Base (RIB).

Examples

The following is sample output from the show ip route database command:

```
Switch# show ip route database
```

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

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

[*] - [AD/Metric]

> - selected route, * - FIB route, p - stale info

```
O    *> 1.1.1.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:48:58
```

```
O    *> 2.2.2.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
```

```
S      6.6.6.0/24 [1/0] via 3.3.3.3 inactive
C      *> 10.10.1.0/24 is directly connected, eth-0-23
C      *> 10.10.1.23/32 is in local loopback, eth-0-23
O      *> 10.10.2.0/24 [110/2] via 10.10.1.1, eth-0-23, 00:32:07
O      *> 10.10.3.0/24 [110/3] via 10.10.1.1, eth-0-23, 00:32:07
```

Related Commands

ip route
show ip route

6.1.11 show ip protocols

Command Purpose

To display the parameters and current state of the active routing protocol process, use the show ip protocols command in privileged EXEC mode.

Command Syntax

show ip protocols (*vrf NAME* |) (*PROTOCOL* |)

Parameter	Parameter Description	Parameter Value
VRF NAME	VRF instance name	A string up to 15 characters
PROTOCOL	(Optional) The name of a routing protocol. If you specify a routing protocol, use one of the following keywords: bgp, ospf, isis and rip.	bgp/ospf/rip/isis

Command Mode

Privileged EXEC

Default

None

Usage

The information displayed by the show ip protocols command is useful in debugging routing operations. Information in the Routing Information Sources field of the show ip protocols output can help you identify a switch suspected of delivering bad routing information.

Examples

The following is sample output from the show ip protocols command:

```
Switch# show ip protocols
```

Routing Protocol is "ospf 0"

Redistributing:

Routing for Networks:

3.3.3.0/24

10.10.1.0/24

10.10.4.0/24

Distance: (default is 110)

Related Commands

show ip route

6.1.12 show ip route summary

Command Purpose

To display the total route count and different types of route count, use the show ip route summary command in privileged EXEC mode.

Command Syntax

show ip route (*vrf NAME* |) summary

Parameter	Parameter Description	Parameter Value
VRF NAME	VRF instance name	A string up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip route summary command:

```
Switch# show ip route summary
```

```
IP routing table name is Default-IP-Routing-Table(0)
```

```
IP routing table maximum-paths is 8
```

Route source	networks
connected	2
static	1
Total	3

Related Commands

show ip route

6.1.13 show ip route add-fib-fail

Command Purpose

Use this command to display the routes which can not forward packet because of TCAM resource full. Use the show ip route add-fib-fail command in privileged EXEC mode.

Command Syntax

show ip route add-fib-fail (count |)

Parameter	Parameter Description	Parameter Value
count	number of add-fib-fail route entries	-

Command Mode

Privileged EXEC

Default

None

Usage

If both of the command line "show ip route" and "show ip route add-fib-fail" could show the same route. It represents that the route is not able to inset into the Forwarding Information Table(FIB) due to the hareware resource limit, this route is not able to forward any packets. You could delete and reconfigure this routing when some hardware resource is free.

Examples

The following is sample output from the show ip route add-fib-fail command:

```
Switch# show ip route add-fib-fail
```

```
=====
VRF      Route
default  1.1.1.1/32
```

default	1.1.1.0/24
test	2.2.2.2/32
test	2.2.2.0/24

Related Commands

show ip route

6.1.14 max-static-routes

Command Purpose

To configure the maximum static routes in system, use the max-static-routes command in global configuration mode. To configure the maximum static routes to default value, use the no form of this command.

Command Syntax

max-static-routes COUNT

no max-static-routes COUNT

Parameter	Parameter Description	Parameter Value
COUNT	maximum static routes in system	The range is <1-65535>, default value is 1024

Command Mode

Global Configuration

Default

1024

Usage

Users should not configure the maximum static routes more than system profile of FIB. Also, users should not configure the maximum static routes less than the current static routes count.

Examples

The following example displays how to change maximum static routes to 10:

```
Switch# confi terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# max-static-routes 10
```

Related Commands

show ip route summary

6.1.15 show resource fib

Command Purpose

Use this command to display the resources used by routes.

Command Syntax

show resource fib

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource fib command:

```
Switch# show resource fib
```

```
Switch# show resource fib
```

```
RIBFIB
```

Resource	Used	Capability
=====		
Indirect Routes	3	8192
Host Routes	1	4096
Static Routes	0	1024
IPv6 Indirect routes	0	1536
IPv6 Host routes	0	4096
IPv6 Static routes	0	1024

Related Commands

show ip route summary

6.1.16 ecmp load-balance-mode dynamic

Command Purpose

Use this command to configure ecmp dynamic load balance.

Command Syntax

ecmp load-balance-mode dynamic
no ecmp load-balance-mode dynamic

Command Mode

Global Configuration

Default

Static load balance mode

Usage

When configure or cancel ecmp load balance, the route information must be empty.

Examples

The following example displays how to configure ecmp dynamic load balance:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ecmp load-balance-mode dynamic
```

Related Commands

None

6.1.17 ecmp load-balance-mode dynamic (efd-only|tcp-only)

Command Purpose

Use this command to configure only tcp flows do ecmp dynamic load or only efd flows do ecmp dynamic load.

Command Syntax

ecmp load-balance-mode dynamic (efd-only | tcp-only)

no ecmp load-balance-mode dynamic

Command Mode

Global Configuration

Default

Flows of every type can do ecmp dynamic load.

Usage

None

Examples

The following example displays how to configure only tcp flows do ecmp dynamic load:

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)# ecmp load-balance-mode dynamic tcp-only
```

Related Commands

None

6.1.18 ecmp load-balance-mode static

Command Purpose

Use this command to configure ecmp static load balance.

Command Syntax

ecmp load-balance-mode static

Command Mode

Global Configuration

Default

None

Usage

When configure ecmp load balance, the route information must be empty.

Examples

The following example displays how to configure ecmp static load balance:

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# ecmp load-balance-mode static
```

Related Commands

None

6.1.19 ecmp load-balance-mode static self-healing

Command Purpose

Use this command to configure ecmp self-healing load balance.

Command Syntax

ecmp load-balance-mode static self-healing

no ecmp load-balance-mode static self-healing

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example displays how to configure ecmp self-healing load balance:

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# ecmp load-balance-mode static self-healing
```

Related Commands

None

6.1.20 ecmp load-balance-mode round-robin

Command Purpose

Use this command to configure ecmp round robin load balance.

Command Syntax

ecmp load-balance-mode round-robin *A.B.C.D/M*

no ecmp load-balance-mode round-robin *A.B.C.D/M*

Parameter	Parameter Description	Parameter Value
<i>A.B.C.D/M</i>	IP destination prefix (e.g. 10.0.0.0/8), vrf private route isn't support RR	IPv4 address and mask length in A.B.C.D/M format

Command Mode

Global Configuration

Default

None

Usage

When configure or cancel ecmp load balance, the route information must be empty.

Examples

The following example displays how to configure ecmp round robin load balance:

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# ecmp load-balance-mode round-robin 1.1.1.0/24
```

Related Commands

None

6.1.21 show ecmp information

Command Purpose

Use this command to display ecmp configure information.

Command Syntax

show ecmp information

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the output of the command:

```
Switch# show ecmp information
```

```
ECMP load balance enable mode: Static
```

```
ECMP hash-field-select:
```

```
    ipsa ipda
```

```
    inner-ipda
```

Related Commands

None

6.2 RIP Commands

6.2.1 default-information originate (RIP)

Command Purpose

To generate a default route into Routing Information Protocol (RIP), use the default-information originate command in router configuration mode. To disable this feature, use the no form of this command.

Command Syntax

default-information originate (route-map |)

no default-information originate

Parameter	Parameter Description	Parameter Value
route-map	Route map reference	-

Command Mode

Router Configuration

Default

None

Usage

The route originated will only be learned by RIP neighbor, and this route is not configured in FIB.

Examples

The following example originates a default route:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# version 2
Switch(config-router)# network 192.168.16.0/24
Switch(config-router)# default-information originate
```

Related Commands

None

6.2.2 default-metric (RIP)

Command Purpose

To set default metric values for Routing Information Protocol (RIP), use the default-metric command in router configuration mode. To return to the default state, use the no form of this command.

Command Syntax

default-metric *NUMBER-VALUE*

no default-metric

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Default metric value	1-16

Command Mode

Router Configuration

Default

By default, the metric is set to 1.

Usage

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a switch using both the RIP and the Open Shortest Path First (OSPF) routing protocols. The example advertises OSPF-derived routes using RIP and assigns the OSPF-derived routes a RIP metric of 10:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ospf
```

Related Commands

redistribute (RIP)

6.2.3 distance (RIP)

Command Purpose

To define an administrative distance for routes that are inserted into the routing table, use the distance command in router configuration mode. To return the administrative distance to its default distance definition, use the no form of this command.

Command Syntax

```
distance DISTANCE PREFIX/PREFIX-LENGTH ( ACCESS-NAME | )
no distance
```

Parameter	Parameter Description	Parameter Value
DISTANCE	Administrative distance	Administrative distance, an integer from 1 to 255 (routes with a distance value of 255 are not installed in the routing table)
PREFIX	IP prefix for the originator of the incoming routing updates	IPv4 Address
PREFIX-LENGTH	Prefix length for the originator	1-32
ACCESSS-LIST-NAME	(Optional) Named access list to be applied to incoming routing updates	Up to 40 characters

Command Mode

Router Configuration

Default

By default, the distance is 120.

Usage

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual switch or a group of switches. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

When this command is configured, it is applied when a network is being inserted into the routing table. It filters routing updates according to the IP address of the switch that supplies the routing information. It could be used, for example, to filter possibly incorrect routing information from switches that are not under your administrative control. The optional access list name is used to filter router entries in routing update.

Examples

The following example set administrative distance 200 for routes that are inserted from 20.20.0.0 network segment :

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.10.0.0/24
Switch(config-router)# network 20.20.0.0/24
Switch(config-router)# distance 200 20.20.0.0/24
```

Related Commands

distance (OSPF)

6.2.4 ip rip authentication

Command Purpose

To enable authentication for Routing Information Protocol (RIP) Version 2 packets and to specify the set of keys that can be used on an interface, use the `ip rip authentication` command in interface configuration mode. To prevent authentication, use the `no` form of this command.

Command Syntax

`ip rip authentication ( key-chain NAME-OF-CHAIN | string STRING )`

`no ip rip authentication ( key-chain | string )`

Parameter	Parameter Description	Parameter Value
key-chain <i>NAME-OF-CHAIN</i>	Enables authentication and specifies the group of keys that are valid	A String of key chain name
string <i>STRING</i>	Enables authentication and specifies the authentication string	Up to 16 characters

Command Mode

Interface Configuration

Default

No authentication is provided for RIP packets.

Usage

If neither key chain is configured with the `key-chain` command nor string is configured with the `authentication string` command, no authentication is performed on the interface (not even the default authentication). Key chain and authentication string can not be configured on the same interface. If you want configure one, make sure the other is not configured.

Examples

The following example configures the interface to accept and send any key belonging to the key chain named `trees`:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication key-chain trees
```

Related Commands

`ip rip authentication mode`

6.2.5 ip rip authentication mode

Command Purpose

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the `ip rip authentication mode` command in interface configuration mode. To restore clear text authentication, use the `no` form of this command.

Command Syntax

`ip rip authentication mode ( text | md5 )`

`no ip rip authentication mode`

Parameter	Parameter Description	Parameter Value
text	Normal text authentication	-
md5	Keyed Message Digest 5 (MD5) authentication	-

Command Mode

Interface Configuration

Default

Clear text authentication is provided for RIP packets.

Usage

RIP Version 1 does not support authentication.

Examples

The following example configures the interface to use MD5 authentication:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip rip authentication mode md5
```

Related Commands

`ip rip authentication key-chain`

6.2.6 ip rip receive version

Command Purpose

To specify a Routing Information Protocol (RIP) version to receive on an interface basis, use the `ip rip receive version` command in interface configuration mode. To follow the global version rules, use the `no` form of this command.

Command Syntax

`ip rip receive version [ 1 | 2 ]`

`no ip rip receive version`

Parameter	Parameter Description	Parameter Value
1	(Optional) Accepts only RIP Version 1 packets on the interface	-
2	(Optional) Accepts only RIP Version 2 packets on the interface	-

Command Mode

Interface Configuration

Default

Only RIPv2 packet should be received.

Usage

Use this command to override the default behavior of RIP as specified by the `version` command. This command applies only to the interface being configured. You can configure the interface to accept both RIP versions.

Examples

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive version 1 2
```

Related Commands

`version (RIP)`

6.2.7 ip rip receive-packet

Command Purpose

To enable the interface to receive Routing Information Protocol (RIP) packets, use the `ip rip receive-packet` command in interface configuration mode. To disable to receive RIP packets, use the `no` form of this command.

Command Syntax

```
ip rip receive-packet
no ip rip receive-packet
```

Command Mode

Interface Configuration

Default

Receive packet is enabled by default.

Usage

Use this command to enable or disable the capability of receiving RIP packets, whether the network of this interface is added into RIP or not.

Examples

The following example enables the reception of RIP packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip receive-packet
```

Related Commands

```
ip rip receive version
```

6.2.8 ip rip send version

Command Purpose

To specify a Routing Information Protocol (RIP) version to send on an interface basis, use the `ip rip send version` command in interface configuration mode. To follow the global version rules, use the `no` form of this command.

Command Syntax

```
ip rip send version ([ 1 | 2 ]) 1-compatible
no ip rip send version
```

Parameter	Parameter Description	Parameter Value
1	(Optional) Sends only RIP Version 1 packets out the interface	-

Parameter	Parameter Description	Parameter Value
2	(Optional) Sends only RIP Version 2 packets out the interface	-
1-compatible	(Optional) Sends RIP Version 2 packets out the interface with broadcast IP address	-

Command Mode

Interface Configuration

Default

Only RIPv2 packet should be send.

Usage

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. You can configure the interface to send both RIP versions.

Examples

The following example configures the interface to send both RIP Version 1 and Version 2 packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send version 1 2
```

Related Commands

ip rip receive version

6.2.9 ip rip send-packet

Command Purpose

To enable the interface to send Routing Information Protocol (RIP) packets, use the ip rip send-packet command in interface configuration mode. To disable to send RIP packets, use the no form of this command.

Command Syntax

```
ip rip send-packet
no ip rip send-packet
```

Command Mode

Interface Configuration

Default

Send packet is enabled by default.

Usage

Use this command to enable or disable the capability of sending RIP packets, whether the network of this interface is added into RIP or not.

Examples

The following example enables the transmission of RIP packets:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip rip send-packet
```

Related Commands

ip rip send version

6.2.10 ip rip split-horizon

Command Purpose

To enable the split horizon mechanism for Routing Information Protocol (RIP), use the ip rip split-horizon command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command.

Command Syntax

```
ip rip split-horizon (poisoned | )
no ip rip split-horizon
```

Parameter	Parameter Description	Parameter Value
poisoned	Split horizon with poisoned reverse	-

Command Mode

Interface Configuration

Default

This command is enabled with poisoned reverse by default.

Usage

In general, changing the state of the default for the `ip rip split-horizon` command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes.

Examples

The following example enables split horizon without poisoned reverse:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip rip split-horizon
```

Related Commands

None

6.2.11 network (RIP)

Command Purpose

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the `network` command in router configuration mode. To remove an entry, use the `no` form of this command.

Command Syntax

`network ( PREFIX / PREFIX-LENGTH )`

`no network ( PREFIX / PREFIX-LENGTH )`

Parameter	Parameter Description	Parameter Value
PREFIX	IP route prefix for the network	IPv4 Address
PREFIX-LENGTH	Prefix length for the network	1-32

Command Mode

Router Configuration

Default

No networks are specified.

Usage

There is no limit to the number of network commands you can use on the switch. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

Examples

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.99.0.0/16 and 192.168.7.0/24:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.99.0.0/16
Switch(config-router)# network 192.168.7.0/24
```

Related Commands

router rip

6.2.12 neighbor (RIP)

Command Purpose

To define a neighboring switch with which to exchange routing information, use the neighbor command in router configuration mode. To remove an entry, use the no form of this command.

Command Syntax

neighbor *IP-ADDRESS*

no neighbor *IP-ADDRESS*

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	IP address of a peer switch with which routing information will be exchanged	IPv4 Address

Command Mode

Router Configuration

Default

No neighboring switches are defined.

Usage

This command permits the point-to-point (non-broadcast) exchange of routing information. When it is used in combination with the passive-interface router configuration command, routing information can be exchanged between a subset of switches and access servers on a LAN.

Multiple neighbor commands can be used to specify additional neighbors or peers.

Examples

In the following example, RIP updates are sent to all interfaces on network 10.108.0.0 except eth-0-1. However, in this case a neighbor switch configuration command is included. This command permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
Switch(config-router)# neighbor 10.108.20.4
```

Related Commands

router rip

6.2.13 offset-list (RIP)

Command Purpose

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the offset-list command in router configuration mode. To remove an offset list, use the no form of this command.

Command Syntax

offset-list *ACCESSS-LIST-NAME* (in | out) *METRIC-OFFSET* (*IFNAME* |)

no offset-list (in | out) (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
ACCESSS-LIST-NAME	Named access list to be applied	Up to 40 characters
in	Applies the access list to incoming metrics	-
out	Applies the access list to outgoing metrics	-
METRIC-OFFSET	Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken	0-16

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name to which the offset list is applied	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The offset value is added to the routing metric. An offset list with an interface is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the switch applies an offset to the delay component of a switch only to access list 21:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# offset-list 21 out 10
```

Related Commands

None

6.2.14 passive-interface (RIP)

Command Purpose

To disable sending routing updates for the Routing Information Protocol (RIP) on an interface, use the passive-interface command in router configuration mode. To re-enable the sending of routing updates, use the no form of this command.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

Routing updates are sent on the interface.

Usage

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# passive-interface eth-0-1
```

Related Commands

router rip

6.2.15 redistribute (RIP)

Command Purpose

To redistribute routes from one routing domain into RIP routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax

```
redistribute PROTOCOL { [ metric VALUE ] | route-map WORD }
no redistribute PROTOCOL
```

Parameter	Parameter Description	Parameter Value
PROTOCOL	(Optional) The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol, use one of the following keywords: bgp, and ospf, connected,isis	bgp/ospf/connected/isis/static/isis
metric VALUE	(Optional) When redistributing other routing process to the RIP process, the default metric is 1 if no metric value is specified	1-16
route-map	Route map reference	-
WORD	Pointer to route-map entries	Up to 20 characters

Command Mode

Router Configuration

Default

Route redistribution is disabled.

Metric metric-value: 1

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples

The following examples redistribute the static routes into RIP with metric 10:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.108.0.0/16
Switch(config-router)# redistribute static metric 10
```

Related Commands

default-metric

6.2.16 router rip

Command Purpose

To configure the Routing Information Protocol (RIP) routing process, use the router rip command in global configuration mode. To turn off the RIP routing process, use the no form of this command.

Command Syntax

router rip
no router rip

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to enter the RIP routing configuration:

```
Switch# configure terminal  
Switch(config)# router rip
```

Related Commands

network (RIP)

6.2.17 timers basic (RIP)

Command Purpose

To adjust Routing Information Protocol (RIP) network timers, use the timers basic command in router configuration mode. To restore the default timers, use the no form of this command.

Command Syntax

timers basic *UPDATE TIMEOUT INVALID*
no timers basic

Parameter	Parameter Description	Parameter Value
UPDATE	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol.	<5-2147483647>, default 30s

Parameter	Parameter Description	Parameter Value
TIMEOUT	Time (in seconds) after which a route is declared invalid without updates that refresh the route. The route then enters into an invalid state and is not used for forwarding packets.	It is marked inaccessible and advertised as unreachable. <5-2147483647>, default 180s
INVALID	Time after which an invalid route is removed from RIP routing database.	<5-2147483647>, default 120s

Command Mode

Router Configuration

Default

update: 30 seconds

timeout: 180 seconds

invalid: 120 seconds

Usage

The basic timing parameters for RIP are adjustable. Because RIP is executing a distributed, asynchronous routing algorithm, these timers must be the same for all switches and access servers in the network.

In addition, an address family can have explicitly specified timers that apply to that address-family only. The timers basic command must be specified for an address family or the system Default for the timers basic command are used regardless of what is configured for RIP routing.

Examples

The following example sets updates to be broadcast every 5 seconds. If a switch is not heard from in 15 seconds, the route is declared unusable. And after 15 seconds the invalid route will be removed from RIP routing database:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# timers basic 5 15 15
```

Related Commands

None

6.2.18 show ip rip database

Command Purpose

Use this command to display RIP information database.

Command Syntax

show ip rip database (vrf *WORD* |)

Parameter	Parameter Description	Parameter Value
vrf <i>WORD</i>	VPN Routing/Forwarding instance	Up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip database command:

```
Switch# show ip rip database
```

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

Network	Next Hop	Metric From	If	Time
Rc 1.1.1.0/24		1	eth-0-1	
Rc 2.2.2.0/24		1	eth-0-2	
Rc 10.0.0.0/24		1	vlan10	

Related Commands

show ip rip interface

6.2.19 show ip rip interface

Command Purpose

To display summary information of Routing Information Protocol (RIP) for a specific interface, use the show ip rip interface command in privileged EXEC mode.

Command Syntax

show ip rip interface (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support physical/aggregation/loopback/tunnel/vlan interfaces

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip interface command:

```
Switch# show ip rip interface eth-0-1
```

```
eth-0-1 is up, line protocol is up
```

```
  Routing Protocol: RIP
```

```
    Receive RIP packets
```

```
    Send RIP packets
```

```
    Passive interface: Disabled
```

```
    Split horizon: Enabled with Poisoned Reversed
```

```
    IP interface address:
```

```
      1.1.1.1/24
```

Related Commands

show ip rip database

6.2.20 version (RIP)

Command Purpose

To specify a Routing Information Protocol (RIP) version used globally by the router, use the version command in router configuration mode. To restore the default value, use the no form of this command.

Command Syntax

version (1 | 2)

no version

Parameter	Parameter Description	Parameter Value
1	Specifies RIP Version 1	-
2	Specifies RIP Version 2	-

Command Mode

Router Configuration

Default

System receives RIP Version 1 and Version 2 packets, but sends only Version 2 packets.

Usage

To specify RIP versions used on an interface basis, use the ip rip receive version and ip rip send version commands.

Examples

The following example enables the software to send and receive RIP Version 2 packets:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# version 2
```

Related Commands

ip rip receive version

ip rip send version

6.2.21 distribute-list

Command Purpose

To Filter networks in routing updates, use the distribute-list command in router configuration mode. To restore the default value, use the no form of this command.

Command Syntax

distribute-list (prefix |) WORD (in | out)

no distribute-list (prefix |) WORD (in | out)

Parameter	Parameter Description	Parameter Value
prefix	Filter prefixes in routing update	-
WORD	Access-list name	Up to 40 characters

Parameter	Parameter Description	Parameter Value
in	Filter incoming routing updates	-
out	Filter outgoing routing updates	-

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example filters all routes from RIP:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix 1 in
```

Related Commands

ip prefix-list

6.2.22 address-family

Command Purpose

Use the command enter Address Family command mode in router configuration mode.

Command Syntax

address-family ipv4 vrf *WORD*

Parameter	Parameter Description	Parameter Value
WORD	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Router Configuration

Default

N/A

Usage

None

Examples

The following example shows how to enter Address Family command mode:

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router)address-family ipv4
```

Related Commands

None

6.2.23 show ip protocol rip**Command Purpose**

To show Routing Information Protocol (RIP), use the show ip protocol rip command in in privileged EXEC mode.

Command Syntax

```
show ip protocol rip
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip interface command:

```
Switch# show ip protocol rip
```

```
Routing protocol is "rip"
```

```
Sending updates every 30 seconds with +/-5 seconds
```

```
Timeout after 180 seconds, Garbage collect 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:
```

```
connected metric default
```

```
Default version control: send version 2, receive version 2
```

```
Interface      Send      Recv      Key-chain
```

```
Routing for Networks:
```

```
10.10.11.0/24
```

```
Routing Information Sources:
```

```
Gateway      Distance  Last Update  Bad Packets  Bad Routes
```

```
Number of routes (including connected): 0
```

```
Distance: (default is 120)
```

Related Commands

None

6.2.24 debug rip

Command Purpose

Use this command to specify the options for the displayed debugging information for RIP events, RIP packets. Use the no parameter with this command to disable all debugging.

Command Syntax

```
debug rip ( all | events | PACKET | )
```

```
no debug rip ( all | events | PACKET | )
```

```
no debug all ( rip | )
```

Parameter	Parameter Description	Parameter Value
all	All RIP debug information	-
events	RIP events debug information is displayed	-
PACKET	packet (recv send) (detail) Specifies RIP packets only	-
recv	Specifies that information for received packets be displayed	-

Parameter	Parameter Description	Parameter Value
send	Specifies that information for sent packets be displayed	-
detail	Displays detailed information for the sent or received packet	-

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

The following example displays information about the rip packets that are received and sent out from the connected router:

```
Switch# debug rip packet
```

Related Commands

show debugging rip

6.2.25 show debugging rip

Command Purpose

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging.

Command Syntax

show debugging rip

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show debugging rip command:

```
Switch# show debugging rip
```

RIP debugging status:

RIP packet debugging is on

Related Commands

debug rip

6.2.26 show ip rip database database-summary

Command Purpose

Use this command to display the statistics for RIP routes.

Command Syntax

show ip rip database database-summary (vrf *NAME* |)

Parameter	Parameter Description	Parameter Value
vrf <i>NAME</i>	VPN Routing/Forwarding instance	Up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip database database-summary command:

```
Switch# show ip rip database database-summary
```

Type	Count
RIP connected	1
RIP	1
Total	2

Related Commands

```
show ip rip database
```

6.2.27 show resource rip

Command Purpose

Use this command to display the route resources used by RIP protocol.

Command Syntax

```
show resource rip
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource rip command:

```
Switch# show resource rip
```

RIP Resource	Used	Capability
=====		
Routes	2	6144

Related Commands

show ip rip database

6.3 OSPF Commands

6.3.1 area authentication

Command Purpose

To enable authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in router configuration mode. To remove an authentication specification of an area or a specified area from the configuration, use the no form of this command.

Command Syntax

area *AREA-ID* authentication (message-digest |)

no area *AREA-ID* authentication

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument	-

Command Mode

Router Configuration

Default

Type 0 authentication (no authentication)

Usage

Specifying authentication for an area sets the authentication to Type 1 (simple password) as specified in RFC 1247. If this command is not included in the configuration file, authentication of Type 0 (no authentication) is assumed.

The authentication type must be the same for all routers and access servers in an area. The authentication password for all OSPF routers on a network must be the same if they are to communicate with each other via OSPF. Use the ip ospf authentication-key interface command to specify this password.

If you enable MD5 authentication with the message-digest keyword, you must configure a password with the ip ospf message-digest-key interface command.

To remove the authentication specification for an area, use the no form of this command with the authentication keyword.

Examples

The following example mandates authentication for areas 0 and 10.0.0.0 of OSPF routing process 201. Authentication keys are also provided:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.251.201/24
Switch(config-if)# ip ospf authentication-key adcdefgh
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config-if)# ip ospf authentication-key ijklmnop
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0 0.255.255.255 area 10.0.0.0
Switch(config-router)# network 192.168.0.0/16 area 0
Switch(config-router)# area 10.0.0.0 authentication
Switch(config-router)# area 0 authentication
```

Related Commands

ip ospf authentication-key

6.3.2 area default-cost

Command Purpose

To specify a cost for the default summary route sent into a stub, use the area default-cost command in router configuration mode. To remove the assigned default route cost, use the no form of this command.

Command Syntax

area *AREA-ID* default-cost *COST*

no area *AREA-ID* default-cost

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
COST	default cost value	0-16777214

Command Mode

Router Configuration

Default

COST: 1

Usage

The command is used only on an Area Border Router (ABR) attached to a stub.

There are two stub area router configuration commands: the stub and default-cost options of the area command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the default-cost option only on an ABR attached to the stub area. The default-cost option provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example shows how to configure a stub area and set its COST value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

Related Commands

None

6.3.3 area filter-list

Command Purpose

To filter prefixes advertised in type 3 link-state advertisements (LSAs) between Open Shortest Path First (OSPF) areas of an Area Border Router (ABR), use the area filter-list command in router configuration mode. To change or cancel the filter, use the no form of this command.

Command Syntax

```
area AREA-ID filter-list ( access ACCESSS-LIST-NAME | prefix PREFIX-LIST-NAME ) ( in | out )
no area AREA-ID filter-list ( access ACCESSS-LIST-NAME | prefix PREFIX-LIST-NAME ) ( in | out )
```

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
access	Indicates that an accesslist is used	-
ACCESSS-LIST-NAME	Name of an access list	A string with 1-20 characters
prefix	Indicates that a prefix list is used	-
PREFIX-LIST-NAME	Name of a prefix list	A string with 1-20 characters
in	Access list or prefix list applied to prefixes advertised to the specified area from other areas	-
out	Access list or prefix list applied to prefixes advertised out of the specified area to other areas	-

Command Mode

Router Configuration

Default

This command has no default behavior.

Usage

With this feature enabled in the "in" direction, all type 3 LSAs originated by the ABR to this area, based on information from all other areas, are filtered by the prefix list. Type 3 LSAs that were originated as a result of the area range command in another area are treated like any other type 3 LSA that was originated individually. Any prefix that does not match an entry in the prefix list is implicitly denied.

With this feature enabled in the "out" direction, all type 3 LSAs advertised by the ABR, based on information from this area to all other areas, are filtered by the prefix list. If the area range command has been configured for this area, type 3 LSAs that correspond to the area range are sent to all other areas, only if at least one prefix in the area range matches an entry in the prefix list.

If all specific prefixes are denied by the prefix list, type 3 LSAs that correspond to the area range command will not be sent to any other area. Prefixes that are not permitted by the prefix list are implicitly denied.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
Switch# configure terminal
Switch(config)# router ospf 201
Switch(config-router)# area 1 filter-list prefix AREA_1 in
```

Related Commands

area range

6.3.4 area range

Command Purpose

To consolidate and summarize routes at an area boundary, use the area range command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

area *AREA-ID* range (*ADDRESS MASK* | *ADDRESS / PREFIX-LENGTH*) (advertise | not-advertise |)

no area *AREA-ID* range (*ADDRESS MASK* | *ADDRESS / PREFIX-LENGTH*)

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
ADDRESS	IPv4 address	IPv4 Address
PREFIX-LENGTH	Prefix length of the address	1-32
advertise	Advertise this range (default)	-
not-advertise	Do not advertise this range	-

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The area range command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.110.201/24
```

```
Switch(config)# interface eth-0-2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.120.201/24
Switch(config)# interface eth-0-3
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.0/8
Switch(config)# router ospf 201
Switch(config-router)# network 192.168.110.0/24 area 0
Switch(config-router)# area 10.0.0.0 range 10.0.0.0/8
Switch(config-router)# area 0 range 192.168.110.0 255.255.0.0
```

Related Commands

None

6.3.5 area stub

Command Purpose

To define an area as a stub area, use the `area stub` command in router configuration mode. To disable this function, use the `no` form of this command.

Command Syntax

`area AREA-ID stub ( no-summary | )`

`no area AREA-ID stub ( no-summary | )`

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area	-

Command Mode

Router Configuration

Default

No stub area is defined.

Usage

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the stub and default-cost options of the area router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Examples

The following example shows how to configure a stub area and set its COST value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 stub
Switch(config-router)# area 10.0.0.0 default-cost 20
```

Related Commands

None

6.3.6 area nssa

Command Purpose

To define an area as a NSSA area, use the area nssa command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

area *AREA-ID* nssa (translator-role (candidate | never | always)) (no-summary |) (no-redistribution |) (default-information-originate { metric *METRIC_VALUE* | metric-type *TYPE-VALUE* }))

no area *AREA-ID* nssa (translator-role |) (no-summary |) (no-redistribution |) (default-information-originate |)

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
candidate	(Optional) Configure the role for ABR in NSSA area as candidate for the translator router	-

Parameter	Parameter Description	Parameter Value
never	(Optional) Configure the role for ABR in NSSA area as non-translator router	-
always	(Optional) Configure the role for ABR in NSSA area as the specified translator router	-
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending Summary LSAs into the NSSA area	-
no-redistribution	(Optional) Prevents an Area Border Router (ABR) from importing routes into the NSSA area	-
default-information-originate	(Optional) Configure an ASBR to send default type 7 LSA into the NSSA area	-
metric METRIC_VALUE	(Optional) Configure metric for the default originate route	0-16777214
metric-type TYPE-VALUE	(Optional) Configure metric type for the default originate route	1-2

Command Mode

Router Configuration

Default

No NSSA area is defined.

Usage

No NSSA area is configured as default. You must configure the area nssa command on all routers and access servers in the NSSA area. There are many similarities between NSSA and stub area, neither of which propagates external routes from other area. The difference is that NSSA area can introduce and propagate external routes to the OSPF autonomous domain, while STUB area can not introduce external routes.

Examples

The following example shows how to configure a NSSA area :

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.56.0.201/16
Switch(config)# router ospf 201
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0
Switch(config-router)# area 10.0.0.0 nssa
```

Related Commands

None

6.3.7 auto-cost

Command Purpose

To control how Open Shortest Path First (OSPF) calculates default metrics for the interface, use the auto-cost command in router configuration mode. To assign cost based only on the interface type, use the no form of this command.

Command Syntax

auto-cost reference-bandwidth *RATE*

no auto-cost reference-bandwidth

Parameter	Parameter Description	Parameter Value
RATE	Rate in Mbps (bandwidth).	1-4294967

Command Mode

Router Configuration

Default

100 Mbps

Usage

The value set by the ip ospf cost command overrides the cost resulting from the auto-cost command. Bandwidth dividing port rate is cost.

Examples

The following example changes the cost of the cost link to 1GBps:

```
Switch# configure terminal
```

```
Switch(config)# router ospf 1
```

```
Switch(config-router)# auto-cost reference-bandwidth 1000
```

Related Commands

ip ospf cost

6.3.8 clear ip ospf

Command Purpose

To clear redistribution based on the Open Shortest Path First (OSPF) routing process ID, use the clear ip ospf command in privileged EXEC mode.

Command Syntax

clear ip ospf (*PID* |) process

Parameter	Parameter Description	Parameter Value
PID	(Optional) Process ID	0-65535

Command Mode

Privileged EXEC

Default

None

Usage

Use the PID argument to clear only one OSPF process. If the PID argument is not specified, all OSPF processes are cleared.

Examples

The following example clears all OSPF processes:

```
Switch# clear ip ospf process
```

Related Commands

None

6.3.9 compatible rfc1583

Command Purpose

To restore the method used to calculate summary route costs per RFC 1583, use the compatible rfc1583 command in router configuration mode. To disable RFC 1583 compatibility, use the no form of this command.

Command Syntax

compatible rfc1583

no compatible rfc1583

Command Mode

Router Configuration

Default

Not compatible with RFC 1583.

Usage

To minimize the chance of routing loops, all Open Shortest Path First (OSPF) routers in an OSPF routing domain should have RFC compatibility set identically.

Because of the introduction of RFC 2328, OSPF Version 2, the method used to calculate summary route costs has changed. Use the no compatible rfc1583 command to enable the calculation method used per RFC 2328.

Examples

The following example specifies that the router process is compatible with RFC 1583:

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# compatible rfc1583
```

Related Commands

None

6.3.10 default-information originate (OSPF)

Command Purpose

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command in router configuration mode. To disable this feature, use the no form of this command.

Command Syntax

default-information originate (route-map *WORD* | always | metric *METRIC-VALUE* | metric-type *TYPE-VALUE* |)

no default-information originate (route-map *WORD* | always | metric | metric-type |)

Parameter	Parameter Description	Parameter Value
always	(Optional) Always advertises the default route regardless of whether the system has a default route	-

Parameter	Parameter Description	Parameter Value
metric METRIC-VALUE	metric-value (Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 1.	0-16777214
metric-type TYPE-VALUE	(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be type 1 or type 2 LSA	1-2
route-map WORD	Route map reference	A string with 1-20 characters

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the switch automatically becomes an autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The system still must have a default route for itself before it generates one, except when you have specified the always keyword.

Examples

The following example specifies a metric for the default route redistributed into the OSPF routing domain and an external metric type:

```
Switch# configure terminal
Switch(config)# router ospf 109
Switch(config-router)# redistribute rip metric 100
Switch(config-router)# default-information originate metric 100 metric-type 1
```

Related Commands

redistribute (OSPF)

6.3.11 default-metric (OSPF)

Command Purpose

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command in router configuration mode. To return to the default state, use the no form of this command.

Command Syntax

default-metric METRIC-VALUE

no default-metric (*METRIC-VALUE* |)

Parameter	Parameter Description	Parameter Value
METRIC-VALUE	Default metric value appropriate for the specified routing protocol.	0-16777214

Command Mode

Router Configuration

Default

20

Usage

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes.

Examples

The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP metric of 10.:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute rip
```

Related Commands

redistribute (OSPF)

6.3.12 distance (OSPF)

Command Purpose

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the distance command in router configuration mode. To restore the default value, use the no form of this command.

Command Syntax

```
distance { DISTANCE | ospf [ external DIST1 ] [ inter-area DIST2 ] [ intra-area DIST3 ] }
```

```
no distance { DISTANCE | ospf }
```

Parameter	Parameter Description	Parameter Value
DISTANCE	Administrative distance. An integer from 1 to 255. (Routes with a distance value of 255 are not installed in the routing table.)	1-255
external DIST1	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255.	1-255
inter-area DIST2	(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255.	1-255
intra-area DIST3	(Optional) Sets the distance for all routes within an area. Range is 1 to 255.	1-255

Command Mode

Router Configuration

Default

DIST1: 110

DIST2: 110

DIST3: 110

Usage

You may specify one of the keywords or use distance only to apply to all types of routes.

The distance command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the distance command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Examples

The example advertises OSPF-derived routes using RIP and assigns the Internal Gateway Protocol (IGP)-derived routes a RIP distance of 90:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# distance 90
Switch(config-router)# redistribute rip
```

Related Commands

None

6.3.13 distribute-list (OSPF)

Command Purpose

To filter networks received in updates or suppress networks from being advertised in updates, use the distribute-list command in router configuration mode. To cancel this function, use the no form of this command.

Command Syntax

distribute-list *ACCESSS-LIST-NAME* (in | out)

no distribute-list *ACCESSS-LIST-NAME* (in | out)

Parameter	Parameter Description	Parameter Value
ACCESSS-LIST-NAME	Name of an access list to be applied	A string with 1-20 characters
in	Filter networks received in updates	-
out	Suppress networks from being advertised in updates	-

Command Mode

Router Configuration

Default

None

Usage

This command must specify an access list.

Examples

In the following example, OSPF process 1 is configured to accept two networks, network 20.0.0.0 and network 10.108.0.0:

```
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-ip-acl)# permit any 20.0.0.0 0.0.255.255 any
Switch(config-ip-acl)# permit any 10.108.0.0 0.0.255.255 any
Switch(config-ip-acl)# deny any any any
Switch(config)# router ospf 1
Switch(config-router)# network 10.108.0.0/16 area 1
Switch(config-router)# distribute-list acl1 in
```

Related Commands

ip access-list

6.3.14 ip ospf authentication

Command Purpose

To specify the authentication type for an interface, use the `ip ospf authentication` command in interface configuration mode. To remove the authentication type for an interface, use the `no` form of this command.

Command Syntax

`ip ospf authentication ( message-digest | null | )`

`no ip ospf authentication`

Parameter	Parameter Description	Parameter Value
message-digest	(Optional) Specifies that message-digest authentication will be used	-
null	(Optional) No authentication is used. Useful for overriding password or message-digest authentication if configured for an area	-

Command Mode

Interface Configuration

Default

The area default is no authentication (null authentication).

Usage

Before using the `ip ospf authentication` command, configure a password for the interface using the `ip ospf authentication-key` command. If you use the `ip ospf authentication message-digest` command, configure the message-digest key for the interface with the `ip ospf message-digest-key` command.

Examples

The following example enables message-digest authentication:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip ospf authentication message-digest
```

Related Commands

area authentication
ip ospf authentication-key
ip ospf message-digest-key

6.3.15 ip ospf authentication-key

Command Purpose

To assign a password to be used by neighboring routers that are using the Open Shortest Path First (OSPF) simple password authentication, use the ip ospf authentication-key command in interface configuration mode. To remove a previously assigned OSPF password, use the no form of this command.

Command Syntax

ip ospf authentication-key (8 |) *PASSWORD*
no ip ospf authentication-key

Parameter	Parameter Description	Parameter Value
PASSWORD	Any continuous printable string of characters that can be entered from the keyboard up to 8 bytes in length	A string with 8 characters
(8)	Specifies a hidden password will follow	-

Command Mode

Interface Configuration

Default

No password is specified.

Usage

The password created by this command is used as a "key" that is inserted directly into the OSPF header when the switch originates routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

Examples

The following example enables the authentication key with the string yourpass:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
```



```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip ospf authentication-key yourpass
```

The following example enables the authentication key with the encrypt password 91c38996a1aa5699:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-2
```

```
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip ospf authentication-key 8 91c38996a1aa5699
```

Related Commands

area authentication

ip ospf authentication

6.3.16 ip ospf cost

Command Purpose

To explicitly specify the cost of sending a packet on an interface, use the `ip ospf cost` command in interface configuration mode. To reset the path cost to the default value, use the `no` form of this command.

Command Syntax

```
ip ospf cost INTERFACE-COST
```

```
no ip ospf cost
```

Parameter	Parameter Description	Parameter Value
INTERFACE-COST	The cost of sending a packet on an interface	1-65535

Command Mode

Interface Configuration

Default

Different port rate has different default cost.

Usage

You can set the metric manually using this command, if you need to change the default. Using the `bandwidth` command changes the link cost as long as this command is not used.

Examples

The following example sets the interface cost value to 65:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf cost 65
```

Related Commands

auto-cost reference bandwidth

6.3.17 ip ospf database-filter all out

Command Purpose

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the `ip ospf database-filter all out` command in interface configuration mode. To restore the forwarding of LSAs to the interface, use the `no` form of this command.

Command Syntax

```
ip ospf database-filter all out
no ip ospf database-filter
```

Command Mode

Interface Configuration

Default

This command is disabled by default. All outgoing LSAs are flooded to the interface.

Usage

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use the `database-filter` command to block flooding of LSAs over specified interfaces.

Examples

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through the interface `eth-0-1`:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf database-filter all out
```

Related Commands

None

6.3.18 ip ospf dead-interval

Command Purpose

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

Command Syntax

ip ospf dead-interval *SECONDS*

no ip ospf dead-interval

Parameter	Parameter Description	Parameter Value
SECONDS	The interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down. The value must be the same for all nodes on the network	1-65535

Command Mode

Interface Configuration

Default

SECONDS: The neighbor has been considered as dead in 40s by default.

Usage

The dead interval is advertised in OSPF hello packets. This value must be the same for all networking devices on a specific network. Specifying a smaller dead interval (seconds) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

Examples

The following example sets the OSPF dead interval to 20 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf dead-interval 20
```

Related Commands

ip ospf hello-interval
show ip ospf interface

6.3.19 ip ospf hello-interval

Command Purpose

To specify the interval between hello packets that the switch sends on the interface, use the ip ospf hello-interval command in interface configuration mode. To return to the default time, use the no form of this command.

Command Syntax

ip ospf hello-interval *SECONDS*
no ip ospf hello-interval

Parameter	Parameter Description	Parameter Value
SECONDS	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The range is 1 to 65535. The value must be the same for all nodes on the network	1-65535

Command Mode

Interface Configuration

Default

10 seconds (Ethernet)
30 seconds (non-broadcast)

Usage

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
```

```
Switch(config-if)# ip ospf hello-interval 15
```

Related Commands

ip ospf dead-interval

6.3.20 ip ospf message-digest-key md5

Command Purpose

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the `ip ospf message-digest-key` command in interface configuration mode. To remove an old MD5 key, use the `no` form of this command.

Command Syntax

```
ip ospf message-digest-key KEY-ID md5 ( 8 | ) KEY
```

```
no ip ospf message-digest-key KEY-ID
```

Parameter	Parameter Description	Parameter Value
KEY-ID	An identifier in the range from 1 to 255	1-255
(8)	Specifies a hidden password will follow	-
KEY	Alphanumeric password of up to 16 bytes	A string with 1-16 characters

Command Mode

Interface Configuration

Default

OSPF MD5 authentication is disabled.

Usage

All routers access the same network/sub network share the same password when using this type of authentication. For every OSPF packet, the password is used for generating/examining the "message digest" which is at the tail of the OSPF packet. This "message digest" is processed by OSPF packet and password. There may multiple password be activated on the same interface, this command line always used to transit smoothly to the new password from the old one.

Examples

The following example sets a new key 19 with the password 8ry4222:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
```

```
Switch(config-if)# no switchport
Switch(config-if)# ip ospf message-digest-key 10 md5 xvv560qle
Switch(config-if)# ip ospf message-digest-key 19 md5 8ry4222
```

The following example sets a new key 2 with the encrypt password 91c38996a1aa5699:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf message-digest-key 2 md5 8 91c38996a1aa5699
```

Related Commands

area authentication
service password-encryption
ip ospf authentication

6.3.21 ip ospf mtu

Command Purpose

To set the MTU value when sending Database Descriptor (DD) packets, use the `ip ospf mtu` command in interface configuration mode. To restore a default value, use the `no` form of this command.

Command Syntax

```
ip ospf mtu MTU-VALUE
no ip ospf mtu
```

Parameter	Parameter Description	Parameter Value
MTU-VALUE	MTU value	576-65535

Command Mode

Interface Configuration

Default

1500

Usage

Whenever OSPF constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value overriding the actual interface MTU size.

This command allows an administrator to configure the MTU size recognized by the OSPF protocol. It does not configure the MTU settings on the kernel. OSPF will not recognize MTU size configuration changes made to the kernel until the MTU size is updated through the CLI.

Examples

The following example sets a new MTU value when sending OSPF DD packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf mtu 1280
```

Related Commands

ip ospf mtu-ignore

6.3.22 ip ospf mtu-ignore

Command Purpose

To disable Open Shortest Path First (OSPF) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DD) packets, use the ip ospf mtu-ignore command in interface configuration mode. To reset to default, use the no form of this command.

Command Syntax

```
ip ospf mtu-ignore
no ip ospf mtu-ignore
```

Command Mode

Interface Configuration

Default

OSPF MTU mismatch detection is enabled.

Usage

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DD packets. If the receiving MTU in the DD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DD packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport
Switch(config-if)# ip ospf mtu-ignore
```

Related Commands

ip ospf mtu

6.3.23 ip ospf priority

Command Purpose

To set the router priority, which helps determine the designated router for this network, use the ip ospf priority command in interface configuration mode. To return to the default value, use the no form of this command.

Command Syntax

ip ospf priority *NUMBER-VALUE*

no ip ospf priority

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	A number value that specifies the priority of the router.	0-255

Command Mode

Interface Configuration

Default

Priority of 1

Usage

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First (OSPF) for non-broadcast networks using the neighbor router configuration command for OSPF.

Examples

The following example sets the router priority value to 4:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
```



```
Switch(config-if)# ip ospf priority 4
```

Related Commands

ip ospf network
neighbor (OSPF)

6.3.24 ip ospf retransmit-interval

Command Purpose

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ip ospf retransmit-interval command in interface configuration mode. To return to the default value, use the no form of this command.

Command Syntax

ip ospf retransmit-interval *SECONDS*
no ip ospf retransmit-interval

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) between retransmissions. The default is 5 seconds	1-65535 seconds

Command Mode

Interface Configuration

Default

5 seconds

Usage

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf retransmit-interval 8
```

Related Commands

None

6.3.25 ip ospf transmit-delay

Command Purpose

To set the estimated time required to send a link-state update packet on the interface, use the `ip ospf transmit-delay` command in interface configuration mode. To return to the default value, use the `no` form of this command.

Command Syntax

`ip ospf transmit-delay SECONDS`

`no ip ospf transmit-delay`

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) between retransmissions. The default is 5 seconds	1-65535

Command Mode

Interface Configuration

Default

1 second

Usage

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip ospf transmit-delay 3
```

Related Commands

None

6.3.26 ip ospf network

Command Purpose

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for a given medium, use the `ip ospf network` command in interface configuration mode. To return to the default value, use the `no` form of this command.

Command Syntax

`ip ospf network ( broadcast | non-broadcast | point-to-multipoint [ non-broadcast ] | point-to-point )`

`no ip ospf network`

Parameter	Parameter Description	Parameter Value
broadcast	Sets the network type to broadcast.(Such as Ethernet,FDDI)	-
non-broadcast	Sets the network type to non-broadcast multi-access (NBMA)	-
point-to-multipoint	Sets the network type to point-to-multipoint.	-
point-to-point	Sets the network type to point-to-point	-

Command Mode

Interface Configuration

Default

Depends on the network type.

Usage

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure non-broadcast multi-access networks as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or non-broadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, there are other configurations where this assumption is not true. For example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, this command will be ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to non-broadcast networks:

On point-to-multipoint, broadcast networks, you can use the neighbor command, and you must specify a cost to that neighbor.

On point-to-multipoint, non-broadcast networks, you must use the neighbor command to identify neighbors. Assigning a cost to a neighbor is optional.

Examples

The following example sets your OSPF network as a non-broadcast network:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.77.17/24
Switch(config-if)# ip ospf network non-bradcast
```

Related Commands

Neighbor (OSPF)

6.3.27 neighbor (OSPF)

Command Purpose

To configure Open Shortest Path First (OSPF) routers interconnecting to non-broadcast networks, use the neighbor command in router configuration mode. To remove a configuration, use the no form of this command.

Command Syntax

neighbor *IP_ADDR* { priority *NUMBER* | poll-interval *SECONDS* }

neighbor *IP_ADDR* (cost *COST* |)

no neighbor *IP_ADDR* { priority *NUMBER* | poll-interval *SECONDS* }

no neighbor *IP_ADDR* (cost *COST* |)

Parameter	Parameter Description	Parameter Value
IP_ADDR	Interface IP address of the neighbor	IPv4 Address
priority NUMBER	(Optional) A number that indicates the router priority value of the non-broadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces	0-255

Parameter	Parameter Description	Parameter Value
poll-interval SECONDS	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.	1-65535 seconds
cost COST	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to non-broadcast multi-access (NBMA) networks	1-65535

Command Mode

Router Configuration

Default

No configuration is specified.

Usage

One neighbor entry must be included in the switch configuration for each known non-broadcast network neighbor. The neighbor address must be the the primary address of the interface.

If a neighboring router has become inactive (hello packets have not been received for the Router Dead Interval period), it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the router first starts up, it sends only hello packets to those routers with nonzero priority, that is, routers that are eligible to become designated routers (DRs) and backup designated routers (BDRs). After the DR and BDR are selected, DR and BDR will then start sending hello packets to all neighbors in order to form adjacencies.

Examples

The following example declares a router at address 192.168.3.4 on a non-broadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# neighbor 192.168.3.4 priority 1 poll-interval 180
```

Related Commands

ip ospf priority

6.3.28 network area (OSPF)

Command Purpose

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the network area command in router configuration mode. To disable OSPF routing for interfaces defined with the address wildcard-mask pair, use the no form of this command.

Command Syntax

network { *IP_ADDR WILDCARD-MASK* | *IP-ADDRESS/PREFIX-LENGTH* } area *AREA-ID*

no network { *IP-ADDRESS WILDCARD-MASK* | *IP-ADDRESS/PREFIX-LENGTH* } area *AREA-ID*

Parameter	Parameter Description	Parameter Value
IP_ADDR	Interface IP address of the neighbor	IPv4 Address
WILDCARD-MASK	IP-address-type mask that includes "don't care" bits	IPv4 mask
PREFIX-LENGTH	Prefix length for the network	1-32
AREA-ID	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address	IP address or number in the range of 0-4294967295

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The IP-ADDRESS and WILDCARD-MASK arguments together allow you to define one or multiple interfaces to be associated with a specific OSPF area using a single command.

Examples

The following partial example initializes OSPF routing process 109, and defines four OSPF areas 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for all other networks:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.108.20.1/24
Switch(config)# router ospf 109
```

```
Switch(config-router)# network 10.108.20.0/24 area 10.9.50.0
Switch(config-router)# network 10.108.0.0/16 area 2
Switch(config-router)# network 10.109.10.0/24 area 3
Switch(config-router)# network 0.0.0.0/0 area 0
```

Related Commands

router ospf

6.3.29 overflow database external

Command Purpose

Use this command to configure the size of the external database and the time the router waits before its entries to exit the overflow state. Use the no parameter with this command to revert to default.

Command Syntax

overflow database external *MAXLSAS RECOVERTIME*

no overflow database external

Parameter	Parameter Description	Parameter Value
MAXLSAS	The maximum number of LSAs. Note that this value should be the same	0-2147483647
RECOVERTIME	The number of seconds the router waits before trying to exit the database	0-65535

Command Mode

Router Configuration

Default

None.

Usage

Use this command to limit the number of AS-external-LSAs a router can receive, once it is in the wait state. It takes the number of seconds specified as the RECOVERTIME to recover from this state.

Examples

The following example shows setting the maximum number of LSAs and the time to recover from overflow state:

```
Switch# configure terminal
Switch(config)# router ospf 200
```

```
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# overflow database external 5 3
```

Related Commands

router ospf

6.3.30 passive-interface (OSPF)

Command Purpose

To disable sending routing updates for the Open Shortest Path First (OSPF) on an interface, use the passive-interface command in router configuration mode. To re-enable the sending of routing updates, use the no form of this command.

Command Syntax

passive-interface *IFNAME*

no passive-interface *IFNAME*

Parameter	Parameter Description	Parameter Value
<i>IFNAME</i>	The interface name	Support physical/aggregation/loopback/tu nnel/vlan interfaces

Command Mode

Router Configuration

Default

Routing updates are sent on the interface.

Usage

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

```
Switch# configure terminal
Switch(config)# router ospf 200
Switch(config-router)# network 10.108.0.0/16 area 0
Switch(config-router)# passive-interface eth-0-1
```


Related Commands

router ospf

6.3.31 redistribute (OSPF)

Command Purpose

To redistribute routes from one routing domain into Open Shortest Path First (OSPF) routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax

redistribute *PROTOCOL* [route-map *WORD*] [tag *TAG-VALUE*] [metric *METRIC-VALUE*] [metric-type *TYPE-VALUE*]

no redistribute *PROTOCOL* [metric *METRIC-VALUE*] [metric-type *TYPE-VALUE*]

Parameter	Parameter Description	Parameter Value
route-map <i>WORD</i>	Route map reference.	A string with 1-20 characters
<i>PROTOCOL</i>	(Optional) The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol	use one of the following keywords: static, connected, bgp, and rip
tag <i>TAG-VALUE</i>	Set tag for routes redistributed into OSPF	0-4294967295
metric <i>METRIC-VALUE</i>	(Optional) When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified	0-16777214
metric-type <i>TYPE-VALUE</i>	For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values	1-2

Command Mode

Router Configuration

Default

Route redistribution is disabled.

metric metric-value: 20

metric-type TYPE-VALUE: Type 2 external route

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples

The following example redistribute the static routes into OSPF with metric 10:

```
Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# network 10.108.0.0/16 area 100
Switch(config-router)# redistribute static metric 10
```

Related Commands

default-metric

6.3.32 router-id (OSPF)

Command Purpose

To use a fixed router ID, use the router-id command in router configuration mode. To force Open Shortest Path First (OSPF) to use the previous OSPF router ID behavior, use the no form of this command.

Command Syntax

router-id *IP_ADDR*

no router-id

Parameter	Parameter Description	Parameter Value
IP_ADDR	Router ID in IP address format	IPv4 Address

Command Mode

Router Configuration

Default

No OSPF routing process is defined.

Usage

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the clear ip ospf command.

Examples

The following example specifies a fixed router-id:

```
Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# router-id 10.1.1.1
```

Related Commands

```
clear ip ospf
router ospf
```

6.3.33 router ospf

Command Purpose

To configure an Open Shortest Path First (OSPF) routing process, use the `router ospf` command in global configuration mode. To terminate an OSPF routing process, use the `no` form of this command.

Command Syntax

```
router ospf [ PROCESS-ID [ vrf VPN-NAME ] ]
no router ospf [ PROCESS-ID ]
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPF routing process.If you don't assign a PROCESS-ID, it enter process ID 0. Process ID 0 will be closed if you use the no form of this command and don't assign PORCESS-ID.	1-65535
vrf VPN-NAME	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes	A string with 1-15 characters

Command Mode

Global Configuration

Default

No OSPF routing process is defined.

Usage

You can specify multiple OSPF routing processes in each router. If you do not specify the process-id, the process-id will be the default 0.

Examples

The following example configures an OSPF routing process and assign a process number of 109:

```
Switch# configure terminal
Switch(config)# router ospf 109
Switch(config-router)#
```

Related Commands

network area

6.3.34 summary-address (OSPF)

Command Purpose

To create aggregate addresses for Open Shortest Path First (OSPF), use the summary-address command in router configuration mode. To restore the default, use the no form of this command.

Command Syntax

summary-address *PREFIX/PREFIX-LENGTH* (not-advertise | tag *TAG-VALUE* |)

no summary-address *PREFIX/PREFIX-LENGTH* (not-advertise | tag *TAG-VALUE* |)

Parameter	Parameter Description	Parameter Value
PREFIX	IP route prefix for the destination	IPv4 Address
PREFIX-LENGTH	Prefix length for the network	1-32
not-advertise	(Optional) Suppress routes that match the specified prefix/mask pair. This keyword applies to OSPF only	-
tag TAG-VALUE	Route tag value. The default tag is 0.	0-4294967295

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the largest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization between OSPF areas.

OSPF does not support the summary-address 0.0.0.0/0 command.

Examples

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# summary-address 10.1.0.0/16
```

Related Commands

area range

6.3.35 show ip ospf

Command Purpose

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command in user EXEC or privileged EXEC mode.

Command Syntax

show ip ospf (*PROCESS-ID* |)

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process	0-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip ospf command:

Switch# show ip ospf

```
Routing Process "ospf 100" with ID 11.11.11.11
Process uptime is 0 minute
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 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 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 1
Number of LSA received 3
Number of areas attached to this router: 1
  Area 1
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm last executed 00:00:38.995 ago
    SPF algorithm executed 1 times
    Number of LSA 4. Checksum 0x0235ff
```

Related Commands

None

6.3.36 show ip ospf border-routers

Command Purpose

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the `show ip ospf border-routers` command in privileged EXEC mode.

Command Syntax

`show ip ospf border-routers`

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip ospf border-routers command:

```
Switch# show ip ospf border-routers
```

```
OSPF process 100 internal Routing Table
```

```
Codes: i - Intra-area route, I - Inter-area route
```

```
i 22.22.22.22 [1] via 172.10.1.2, eth-0-10, ABR, Area 1
```

Related Commands

None

6.3.37 show ip ospf database

Command Purpose

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the show ip ospf database command in EXEC mode.

Command Syntax

```
show ip ospf ( PROCESS-ID | ) database database-summary
```

```
show ip ospf ( PROCESS-ID | ) database ( self-originate | max-age | adv-router IP_ADDR | )
```

```
show ip ospf ( PROCESS-ID | ) database ( asbr-summary | external | network | router | summary | nssa-external | opaque-link | opaque-area |  
opaque-as ) ( self-originate | adv-router IP_ADDR | )
```

```
show ip ospf ( PROCESS-ID | ) database ( asbr-summary | external | network | router | summary | nssa-external | opaque-link | opaque-area |  
opaque-as ) LINK-STATE-ID ( self-originate | adv-router A.B.C.D | ) ]
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process	1-65535
adv-router IP_ADDR	(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate)	IPv4 Address
LINK-STATE-ID	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address	IPv4 Address
asbr-summary	(Optional) Displays information only about the autonomous system boundary router summary LSAs	-
external	(Optional) Displays information only about the external LSAs	-
network	(Optional) Displays information only about the network LSAs	-
router	(Optional) Displays information only about the router LSAs	-
self-originate	(Optional) Displays only self-originated LSAs from the local router	-
summary	(Optional) Displays information only about the summary LSAs	-
nssa-external	(Optional) Displays information only about the nssa-external LSAs	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip ospf database command when no arguments or keywords are used:

```
Switch# show ip ospf database
```


Router Link States (Area 3 [Stub])					
Link ID	ADV Router	Age	Seq#	CkSum	Link count
10.0.0.1	10.0.0.1	546	0x80000089	0x4567	1

Related Commands

None

6.3.38 show ip ospf interface

Command Purpose

To display Open Shortest Path First (OSPF)-related interface information, use the show ip ospf interface command in EXEC mode.

Command Syntax

show ip ospf interface (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included	Support physical/aggregation/loopback/tunnel/vlan interfaces

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output of the show ip ospf interface command when eth-0-3 is specified:

```
Switch# show ip ospf interface eth-0-3
```

```
eth-0-3 is up, line protocol is up
```

```
Internet Address 3.3.3.1/24, Area 3 [Stub], MTU 1500
```

```
Process ID 0, Router ID 10.0.0.1, Network Type NBMA, Cost: 1
```

```
Transmit Delay is 1 sec, State DR, Priority 1
```

```
Designated Router (ID) 10.0.0.1, Interface Address 3.3.3.1
```

```
No backup designated router on this network
```

```
Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
Hello due in 00:00:17
Neighbor Count is 1, Adjacent neighbor count is 0
Crypt Sequence Number is 1218176990
Hello received 0 sent 80, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

Related Commands

None

6.3.39 show ip ospf neighbor

Command Purpose

To display Open Shortest Path First (OSPF)-neighbor information on a per-interface basis, use the `show ip ospf neighbor` command in privileged EXEC mode.

Command Syntax

```
show ip ospf neighbor [ IFNAME ] [ NEIGHBOR-ID ] [ detail ] [ all ]
```

Parameter	Parameter Description	Parameter Value
IFNAME	(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included	-
NEIGHBOR-ID	(Optional) Neighbor ID	-
detail	(Optional) Displays all neighbors given in detail (lists all neighbors)	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip ospf neighbor command showing a single line of summary information for each neighbor:

```
Switch# show ip ospf neighbor
```

Neighbor ID	Pri State	Dead Time	Address	Interface
10.199.199.137	1 FULL/DR	0:00:31	192.168.80.37	eth-0-1
172.16.48.1	1 FULL/DROTHER	0:00:33	172.16.48.1	vlan1
172.16.48.200	1 FULL/DROTHER	0:00:33	172.16.48.200	vlan2
10.199.199.137	5 FULL/DR	0:00:33	172.16.48.189	eth-0-2

Related Commands

None

6.3.40 show ip ospf summary-address

Command Purpose

To display the summary addresses redistribution Information used by OSPF, use the show ip ospf summary-address command in privileged EXEC mode.

Command Syntax

```
show ip ospf summary-address
```

Command Mode

Privileged EXEC

Default

None

Usage

Metric equals to 16777215 means not advertise.

Examples

The following example shows how to use show ip ospf summary-address command:

```
Switch# show ip ospf summary-address
```

```
OSPF process 0:
```

```
10.0.0.0/8 Metric 20, Type 2, Tag 0
```

20.0.0.0/8 Metric 16777215, Type 0, Tag 0

Related Commands

None

6.3.41 show ip ospf database database-summary

Command Purpose

To display the summary of database used by OSPF, use the show ip ospf database database-summary command in privileged EXEC mode.

Command Syntax

show ip ospf (*PROCESS-ID* |) database database-summary

Parameter	Parameter Description	Parameter Value
PROCESS-ID	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process	0-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip ospf database database-summary command:

```
Switch# show ip ospf database database-summary
```

OSPF Router with ID (10.10.10.10) (Process ID 0)

Area 0 database summary

LSA Type	Count	MaxAge
Router	1	0
Network	0	0
Summary Net	0	0

Summary ASBR	0	0
Subtotal	1	0
Process 0 database summary		
LSA Type	Count	MaxAge
Router	1	0
Network	0	0
Summary Net	0	0
Summary ASBR	0	0
Type-5 Ext	1	0
Total	2	0

Related Commands

None

6.3.42 show ip ospf route summary

Command Purpose

To display the summary of routes used by OSPF, use the show ip ospf route summary command in privileged EXEC mode.

Command Syntax

show ip ospf (*PROCESS-ID* |) route summary

Parameter	Parameter Description	Parameter Value
PROCESS-ID	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process	0-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip ospf route summary command:

```
Switch# show ip ospf route summary
```

OSPF Router with ID (10.10.10.10) (Process ID 0)

Route Type	Count
(C)Connected	1
(D)Discard	1
(O)Intra area	0
(IA)Inter area	0
(E1)Ext type 1	0
(E2)Ext type 2	0
(N1)NSSA Ext type 1	0
(N2)NSSA Ext type 2	0
Total	2

Related Commands

None

6.3.43 show ip protocols ospf

Command Purpose

To display IP routing protocol process parameters and statistics of Open Shortest Path First (OSPF).use the show ip ospf protocols ospf command in privileged EXEC mode.

Command Syntax

```
show ip protocols ospf ( vrf WORD )
```

Parameter	Parameter Description	Parameter Value
vrf	VPN Routing/Forwarding instance	-
WORD	VPN Routing/Forwarding instance name	A string with 1-15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip protocols ospf command:

```
Switch# show ip protocols ospf
```

```
Routing Protocol is "ospf 0"
```

```
  Redistributing:
```

```
  Routing for Networks:
```

```
  Distance: (default is 110)
```

Related Commands

None

6.3.44 show ip ospf processes-count

Command Purpose

To display the current number and max number of router ospf processes, use the show ip ospf protocols ospf command in privileged EXEC mode.

Command Syntax

```
show ip ospf processes-count
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ip ospf process count:

```
DUT1# show ip ospf processes-count
```

```
OSPF processes current count 0
OSPF processes max count      200
```

Related Commands

None

6.3.45 timers spf

Command Purpose

To set the time of Open Shortest Path First (OSPF) calculating shortest path first (SPF). To restore the default, use the no form of this command.

Command Syntax

timers spf *SPF-START SPF-HOLD*

no timers spf

Parameter	Parameter Description	Parameter Value
SPF-START	Indicates the initial SPF schedule delay in seconds.	0-2147483647
SPF-HOLD	Indicates the minimum hold time between two consecutive SPF calculations.	0-2147483647

Command Mode

Router Configuration

Default

spf-start: 5 seconds

spf-hold: 10 seconds.

Usage

None

Examples

The following example shows a router configured with the start, and hold values for the timers spf command set at 5, and 10 seconds, respectively:

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# router-id 10.10.10.2
```



```
Switch(config-router)#timers spf 5 10
Switch(config-router)# redistribute static
Switch(config-router)# network 10.21.21.0/24 area 0
Switch(config-router)# network 10.22.22.0/24 area 00
```

Related Commands

None

6.3.46 max-concurrent-dd

Command Purpose

To specify Maximum number allowed to process DD concurrently, use the max-concurrent-dd command in router configuration mode. To restore default value, use the no form of this command

Command Syntax

max-concurrent-dd *NUMBER-VALUE*

no max-concurrent-dd

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Number of DD process	1-65535

Command Mode

Router Configuration

Default

5

Usage

None

Examples

The following example shows how to use max-concurrent-dd command:

```
Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10
```

Related Commands

None

6.3.47 maximum-area

Command Purpose

To specify Maximum number of ospf area, use the maximum-area command in router configuration mode. To restore default value, use the no form of this command

Command Syntax

maximum-area *NUMBER-VALUE*

no maximum-area

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Number o f max-area	1-4294967294

Command Mode

Router Configuration

Default

3000

Usage

This command used to specify Maximum number of ospf area.

Examples

The following example shows how to use maximum-area command:

```
Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# maximum-area 100
```

Related Commands

None

6.3.48 refresh timer

Command Purpose

To Set refresh timer of link state database, use the refresh timer command in router configuration mode. To restore default value, use the no form of this command

Command Syntax

refresh timer *NUMBER-VALUE*

no refresh timer (*NUMBER-VALUE*)

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Number of DD process	10-1800

Command Mode

Router Configuration

Default

10 seconds.

Usage

Users are not advised to modify the configuration

Examples

The following example shows how to use refresh timer command:

```
Switch# configure terminal
Switch(config)# router ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# refresh timer 100
```

Related Commands

None

6.3.49 ip ospf bfd

Command Purpose

Use this command to enable IP BFD for ospf on an interface.

Use the "no" form of this command to disable IP BFD for ospf on an interface.

Command Syntax

```
ip ospf bfd
no ip ospf bfd
```

Command Mode

Interface Configuration

Default

By default IP BFD for ospf is disabled on the interface.

Usage

Use this command to enable IP BFD for ospf on an interface.

The IP BFD session should be created when ospf neighbor is created and the neighbor's state is large than "two-way".

The IP BFD session should be destroyed when ospf neighbor is delete or the neighbor's state is not large than "two-way".

Examples

In the following example, IP BFD for ospf is enabled on this interface:

```
Switch# configure terminal
Switch(config-if)# ip ospf bfd
```

Related Commands

None

6.3.50 debug ospf

Command Purpose

Use this command to specify all debugging options for OSPF. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf ( all | )
no debug ospf ( all | )
```

Parameter	Parameter Description	Parameter Value
all	enable all debugging	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf all
```

Related Commands

None

6.3.51 debug ospf events**Command Purpose**

Use this command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax

debug ospf events (abr | asbr | lsa | os | router | vlink |)

no debug ospf events (abr | asbr | lsa | os | router | vlink |)

Parameter	Parameter Description	Parameter Value
abr	Displays ABR events	-
asbr	Displays ASBR events	-
lsa	Displays LSA events	-
os	Displays OS interaction events	-
router	Displays others router events	-
vlink	Displays virtual link events	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf events lsa
```

Related Commands

None

6.3.52 debug ospf ifsm**Command Purpose**

Use this command to specify debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.
Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf ifsm ( status | events | timers | )
```

```
no debug ospf ifsm ( status | events | timers | )
```

Parameter	Parameter Description	Parameter Value
status	Displays IFSM status information	-
events	Displays IFSM event information	-
timers	Displays IFSM TIMER information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf ifsm timers
```

Related Commands

None

6.3.53 debug ospf nfsm

Command Purpose

Use this command to specify debugging options for OSPF Neighbor Finite State Machine (NFSM) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ospf nfsm ( status | events | timers | )
```

```
no debug ospf nfsm ( status | events | timers | )
```

Parameter	Parameter Description	Parameter Value
status	Displays NFSM status information	-
events	Displays NFSM event information	-
timers	Displays NFSM TIMER information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf nfsm timers
```

Related Commands

None

6.3.54 debug ospf lsa

Command Purpose

Use this command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

debug ospf lsa (flooding | generate | install | maxage | refresh |)

no debug ospf lsa (flooding | generate | install | maxage | refresh |)

Parameter	Parameter Description	Parameter Value
flooding	Displays LSA flooding	-
generate	Displays LSA generate	-
install	Displays LSA installation	-
maxage	Displays the maximum age of LSA in seconds	-
refresh	Displays LSA refresh	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf lsa install
```

Related Commands

None

6.3.55 debug ospf packet

Command Purpose

Use this command to specify debugging options for OSPF packets.

Use the no parameter with this command to disable this function..

Command Syntax

debug ospf packet *PARAMETERS*

no debug ospf packet *PARAMETERS*

PARAMETERS = dd | detail | hello | ls-ack | ls-request | ls-update | rcv | send

Parameter	Parameter Description	Parameter Value
dd	Specifies debugging for OSPF database descriptions	-
detail	Sets the debug option to detailed information	-
hello	Specifies debugging for OSPF hello packets	-
ls-ack	Specifies debugging for OSPF link state acknowledgments	-
ls-request	Specifies debugging for OSPF link state requests	-
ls-update	Specifies debugging for OSPF link state updates	-
rcv	Specifies the debug option set for received packets	-
send	Specifies the debug option set for sent packets	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf packet dd send detail
```

Related Commands

None

6.3.56 debug ospf route

Command Purpose

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options.
Use the no parameter with this command to disable this function.

Command Syntax

debug ospf route (ase | ia | install | spf |)

no debug ospf route (ase | ia | install | spf |)

Parameter	Parameter Description	Parameter Value
ase	Specifies the debugging of external route calculation	-
ia	Specifies the debugging of Inter-Area route calculation	-
install	Specifies the debugging of route installation	-
spf	Specifies the debugging of SPF calculation	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug ospf route install
```

Related Commands

None

6.3.57 show debugging ospf

Command Purpose

Use this command to display the set OSPF debugging option..

Command Syntax

show debugging ospf

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the show debugging ospf command:

```
Switch# show debugging ospf
```

OSPF debugging status:

OSPF packet Hello send debugging is on

OSPF packet Database Description send debugging is on

OSPF packet Link State Request send debugging is on

OSPF packet Link State Update send debugging is on

OSPF packet Link State Acknowledgment send debugging is on

OSPF route installation debugging is on

Related Commands

None

6.3.58 show resource ospf**Command Purpose**

Use this command to display the route resources used by OSPF protocol.

Command Syntax

```
show resource ospf
```

Command Mode

Privileged EXEC

Default

None

Usage

If you do not use OSPF, value of capability is 0.

Examples

The following is sample output from the show resource ospf command:

```
Switch# show resource ospf
```

OSPF

Resource	Used	Capability
Routes	1	6144

=====

Routes 1 6144

Related Commands

show ip ospf route summary

6.4 Route Map Commands

6.4.1 route-map

Command Purpose

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing in bgp, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

Command Syntax

```
route-map MAP_TAG ( deny | permit | ) ( SEQUENCE-NUMBER | )
```

```
no route-map MAP_TAG ( deny | permit | ) ( SEQUENCE-NUMBER | )
```

Parameter	Parameter Description	Parameter Value
MAP_TAG	A meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name. The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.	-

Parameter	Parameter Description	Parameter Value
permit	(Optional) If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. (Optional) If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. If the match criteria are not met, and the permit keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.	-
deny	(Optional) If the match criteria are met for the route map and the deny keyword is specified, the route is not redistributed	-
SEQUENCE-NUMBER	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted	1-65535

Command Mode

Global Configuration

Default

The permit keyword is the default.

Usage

None

Examples

The following example shows how to create a route-map and enter route-map configuration mode:

```
Switch# configure terminal
Switch(config)# route-map rip-to-ospf permit
Switch(config-route-map)# match metric 1
Switch(config-route-map)# set metric 2
```

Related Commands

match as-path

match community
 match interface
 match ip address
 match local-preference
 match metric
 match origin
 match route-type
 match tag
 set aggregator
 set as-path
 set atomic-aggregate
 set comm-list
 set community
 set dampening
 set extcommunity
 set ip address
 set local-preference
 set metric
 set metric-type
 set origin
 set originator-id
 set tag
 set vpnv4
 set weight

6.4.2 match as-path

Command Purpose

Use this command to match an autonomous system path access list.

Use the no parameter with this command to remove a path list entry.

The match as-path command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met then the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match as-path *LISTNAME*

no match as-path

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies as autonomous system path access list name	Up to 40 characters

Command Mode

Route-map Configuration

Default

No match as-path is specified by default.

Usage

This command is valid only for BGP.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
```

Related Commands

match metric
match ip address
match community
set as-path
set community

6.4.3 match community

Command Purpose

Use this command to specify the community to be matched.

Use the no parameter with this command to remove the community list entry.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

Use the match community command to allow matching based on community lists.

The values set by the match community command overrides the global values. The route that does not match at least one match clause is ignored.

Command Syntax

match community *WORD*
no match community

Parameter	Parameter Description	Parameter Value
WORD	Specifies the Community-list name	Up to 20 characters

Command Mode

Route-map Configuration

Default

No match community is specified by default.

Usage

This command is valid only for BGP.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist
```

Related Commands

match ip address
match as-path
set as-path
set community
match metric

6.4.4 match interface

Command Purpose

Use this command to define the interface match criterion.

Use the no parameter with this command to remove the specified match criterion..

The match interface command specifies the next-hop interface name of a route to be matched.

Command Syntax

match interface *IFNAME*

no match interface

Parameter	Parameter Description	Parameter Value
IFNAME	A string that specifies the interface for matching	Support physical/aggregation/loopback/tunnel/vlan interfaces

Command Mode

Route-map Configuration

Default

No match interface is specified by default.

Usage

This command is valid only for OSPF.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0/1
```

Related Commands

match tag
match route-type external

6.4.5 match ip address

Command Purpose

Use this command to specify the match address of route.

Use the no parameter with this command to remove the match ip address entry.

The match ip address command specifies the IP address to be matched. If there is a match for the specified IP address, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match ip address *ACCESSLISTID*
no match ip address

Parameter	Parameter Description	Parameter Value
ACCESSLISTID	Specify a IPv4 access-list name, up to 20 characters	-

Command Mode

Route-map Configuration

Default

No match ip address is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ip address List1
```

Related Commands

match community
match as-path
set as-path
set community
match metric

6.4.6 match ip address prefix-list

Command Purpose

Use this command to match entries of prefix-lists.

Use the no parameter with this command to disable this function

This command specifies the entries of prefix-lists to be matched. If there is a match for the specified prefix-list entries, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

```
match ip address prefix-list LISTNAME
no match ip address prefix-list [LISTNAME]
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the IP prefix list name	Up to 40 characters

Command Mode

Route-map Configuration

Default

No match ip address prefix-list is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ip address prefix-list mylist
```

Related Commands

match community
match as-path
set as-path
set community
match metric

6.4.7 match ip next-hop

Command Purpose

Use this command to specify a next-hop address to be matched in a route-map.

Use the no parameter with this command to disable this function.

The match ip next-hop command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match ip next-hop *ACCESSLISTID*

no match ip next-hop [*ACCESSLISTID*]

Parameter	Parameter Description	Parameter Value
ACCESSLISTID	Specify a IPv4 access-list name, up to 20 characters	Up to 40 characters

Command Mode

Route-map Configuration

Default

No match ip next-hop is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ip next-hop mylist
```

Related Commands

match community

match as-path

set as-path

set community

match metric

6.4.8 match ip next-hop prefix-list

Command Purpose

Use this command to specify the next-hop IP address match criterion, using the prefix-list.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax

match ip next-hop prefix-list *LISTNAME*

no match ip next-hop prefix-list [*LISTNAME*]

Parameter	Parameter Description	Parameter Value
LISTNAME	A string specifying the prefix-list name	-

Command Mode

Route-map Configuration

Default

No match ip next-hop prefix-list is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match ip next-hop prefix-list list1
```

Related Commands

match metric
match interface
match ip next-hop

6.4.9 match local-preference

Command Purpose

Use this command to specify the local-preference match criterion.

Use the no parameter with this command to remove the specified match criterion.

Use the match local-preference command to match the local preference of a route.

Command Syntax

match local-preference *LOCAL-PREFERENCE*

no match local-preference

Parameter	Parameter Description	Parameter Value
LOCAL-PREFERENCE	Species the preference value	0-4294967295

Command Mode

Route-map Configuration

Default

No match local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100
```

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

6.4.10 match metric

Command Purpose

Use this command to match a metric of a route.

Use the no parameter with this command to disable this function.

The match metric command specifies the metric to be matched. If there is a match for the specified metric, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match metric *METRICVAL*
no match metric

Parameter	Parameter Description	Parameter Value
METRICVAL	The metric value	0-4294967295

Command Mode

Route-map Configuration

Default

No match metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match metric 2
```

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

6.4.11 match origin

Command Purpose

Use this command to match origin code.

Use the no parameter with this command to disable this matching.

The origin attribute defines the origin of the path information. The **egp** parameter is indicated as an **e** in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The **igp** parameter is indicated as an **i** in the routing table, and it indicates the origin of the path information is interior to the originating AS.

The **incomplete** parameter is indicated as a **?** in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The **match origin** command specifies the origin to be matched. If there is a match for the specified origin, and **permit** is specified, the route is redistributed or controlled as specified by the **set** action. If the match criteria are met, and **deny** is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

```
match origin { egp | igp | incomplete }
```

```
no match origin
```

Parameter	Parameter Description	Parameter Value
egp	learned from EGP	-
igp	Local IGP	-
incomplete	Unknown heritage	-

Command Mode

Route-map Configuration

Default

No match origin is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp
```

Related Commands

None

6.4.12 match route-type external

Command Purpose

Use this command to match specified external route type.

Use the no parameter with this command to turn off the matching.

Use the match route-type external command to match specific external route types. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes, and external type-2 matches only Type 2 external routes.

Command Syntax

```
match route-type external { type-1 | type-2 }
```

```
no match route-type external
```

Parameter	Parameter Description	Parameter Value
type-1	Match OSPF External Type 1 metrics	-
type-2	Match OSPF External Type 1 metrics	-

Command Mode

Route-map Configuration

Default

No match route-type is specified by default.

Usage

This command is valid for OSPF only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1
```

Related Commands

```
match tag
```

6.4.13 match tag

Command Purpose

Use this command to match the specified tag value.

Use the no parameter with this command to turn off the declaration.

Use the match tag command to match the specified tag value.

Command Syntax

match tag *TAG*

no match tag

Parameter	Parameter Description	Parameter Value
TAG	Specifies the tag value	0-4294967295

Command Mode

Route-map Configuration

Default

No match tag is specified by default.

Usage

This command is valid for OSPF RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100
```

Related Commands

match metric

match route-type external

6.4.14 set aggregator

Command Purpose

Use this command to set the AS number for the route map and router ID.

Use the no parameter with this command to disable this function.

An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the set aggregator command to assign an AS number for the aggregator.

To use the set aggregator command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set aggregator as *ASNUM IPADDRESS*

no set aggregator

Parameter	Parameter Description	Parameter Value
ASNUM	Specifies the AS number of aggregator	1-65535
IPADDRESS	Specifies the IP address of aggregator	-

Command Mode

Route-map Configuration

Default

No set aggregator is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set aggregator as 43 10.10.0.3
```

Related Commands

None

6.4.15 set as-path

Command Purpose

Use this command to modify an autonomous system path for a route.

Use the no parameter with this command to disable this function.

Use the set as-path command to specify an autonomous system path. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. this command to prepend an AS path string to routes increasing the AS path length.

To use the set as-path command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set as-path prepend ASN [ ...ASN ]
```

no set as-path

Parameter	Parameter Description	Parameter Value
ASN	System prepends this number to the AS path or overwrite the AS path	1-4294967295

Command Mode

Route-map Configuration

Default

No set as-path is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24
```

Related Commands

None

6.4.16 set atomic-aggregate

Command Purpose

Use this command to set an atomic aggregate attribute.

Use the no parameter with this command to disable this function

To use the set atomic aggregate command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set atomic-aggregate

no set atomic-aggregate

Command Mode

Route-map Configuration

Default

No set atomic-aggregate is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set atomic-aggregate
```

Related Commands

None

6.4.17 set comm-list delete

Command Purpose

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the no parameter with this command to disable this feature.

Command Syntax

set comm-list { *STANDARD_ID* | *EXPANDED_ID* | *WORD* } delete

no set comm-list

Parameter	Parameter Description	Parameter Value
STANDARD_ID	Standard community-list number	1-99
EXPANDED_ID	Expanded community-list number	100-199
WORD	Name of the Community-list	A string with 1-20 characters, the first character should be among [a-zA-Z0-9]
delete	Delete matching communities	-

Command Mode

Route-map Configuration

Default

No set comm-list is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete
```

Related Commands

None

6.4.18 set community

Command Purpose

Use this command to set the communities attribute.

Use the no parameter with this command to delete the entry.

Use this command to set the community attribute and group destinations in a certain community, as well as, apply routing decisions according to those communities.

To use the set community command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set community [AA:NN | internet | local-AS | no-advertise | no-export]

set community none

no set community

Parameter	Parameter Description	Parameter Value
AA:NN	AA:NN: Specifies the community number in this format AA = The AS number NN = The number assigned to community	AA is in the range 1-65535 NN is in the range of 1-65535

Parameter	Parameter Description	Parameter Value
internet	Specifies the Internet (well-known community)	-
local-AS	Specifies no sending outside the local AS (well-known community)	-
no-advertise	Specifies no advertisement of this route to any peer (well-known community)	-
no-export	Specifies no advertisement of this route to next AS (well-known community)	-
none	Removes the community attribute from the prefixes that pass the route-map	-

Command Mode

Route-map Configuration

Default

No set community is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-export no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

Related Commands

None

6.4.19 set dampening

Command Purpose

Use this command to enable route-flap dampening and set parameters.

Use the no parameter with this command to disable it.

Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Command Syntax

set dampening *REACHTIME REUSE SUPPRESS MAXSUPPRESS [UNREACHTIME]*

no set dampening

Parameter	Parameter Description	Parameter Value
REACHTIME	Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes	1-45
REUSE	Specifies the reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750	1-20000
SUPPRESS	Specifies the suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000	1-20000
MAXSUPPRESS	Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes)	1-255
UNREACHTIME	Specifies the un-reachability half-life time for penalty, in minutes. The default value is 15 minutes	1-45

Command Mode

Route-map Configuration

Default

Reference to the syntax description above.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map R1 permit 24
```



```
Switch(config-route-map)# set dampening 20 333 534 30
```

Related Commands

None

6.4.20 set extcommunity

Command Purpose

Use this command to set an extended community attribute.

Use the no parameter with this command to disable this function

To use the set extcommunity command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set extcommunity { rt | soo } EXTCOMMNUMBER [ ...EXTCOMMNUMBER ]
```

```
no set extcommunity { rt | soo }
```

Parameter	Parameter Description	Parameter Value
rt	Specifies the route target of the extended community	-
soo	Specifies the site-of-origin of the extended community	-
EXTCOMMNUMBER	ASN:NN or IP-address nn VPN extended community	-
ASN:NN	the AS number	ASN is in the range 1-65535 NN is in the range of 1-65535
IPADDRESS	the AS number in IP address form	IPv4 Address in A.B.C.D format

Command Mode

Route-map Configuration

Default

No set extcommunity is specified by default.

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 06:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 0.0.0.6:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 06:01
Switch# configure terminal
Switch(config-route-map)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 0.0.0.6:01
```

Related Commands

None

6.4.21 set ip next-hop

Command Purpose

Use this command to set the specified next-hop value.

Use the no parameter with this command to turn off the setting.

Use this command to set the next-hop IP address to the routes.

Command Syntax

set ip next-hop *A.B.C.D* (track *object_id* |)

no set ip next-hop (track |)

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IP address of the next-hop	IPv4 Address in A.B.C.D format
object_id	Object identity is used to identify track object	1-500

Command Mode

Route-map Configuration

Default

No set ip next-hop is specified by default.

Usage

This command is valid for BGP, OSPF, RIP and PBR only. Configuring the set ip next-hop command causes the system to use policy-based routing first and then use the routing table. Configured with track command will bind nexthop with track, when track down, the nexthop will be invalidated. Use the no command with track will unbind nexthop with track.

Examples

The following example shows how to set the next-hop IP address:

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67
```

The following example shows how to set the next-hop IP address and bind with track:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# quit
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ip next-hop 10.10.0.67 track 1
```

Related Commands

None

6.4.22 set ip default next-hop

Command Purpose

Use this command to set the specified default next-hop value.

Use the no parameter with this command to turn off the setting.

Use this command to set the default next-hop IP address to the routes.

Command Syntax

```
set ip default next-hop A.B.C.D ( track object_id | )
```

```
no set ip default next-hop ( track | )
```

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IP address of the default next-hop	IPv4 Address in A.B.C.D format
object_id	Object identity is used to identify track object	1-500

Command Mode

Route-map Configuration

Default

No set ip default next-hop is specified by default.

Usage

This command is valid for PBR only. Configuring the set ip defaultnext-hop command causes the system to use the routing table first and then the policy route to the specified next hop. Configured with track command will bind nexthop with track, when track down, the nexthop will be invalidated. Use the no command with track will unbind nexthop with track.

Examples

The following example shows how to set the default next-hop IP address and bind with track:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0/1 linkstate
Switch(config-track)# quit
Switch(config)# route-map mymap permit 4
Switch(config-route-map)# set ip default next-hop 10.10.0.68 track 1
```

The following example shows how to unbind track with next-hop IP address:

```
Switch# configure terminal
Switch(config)# route-map mymap permit 4
Switch(config-route-map)# no set ip default next-hop track
```

Related Commands

None

6.4.23 set local-preference

Command Purpose

Use this command to set the specified local-preference value.

Use the no parameter with this command to turn off the setting.

Use this command to set the local-preference value of the routes

Command Syntax

set local-preference *LOCAL-PREFERENCE*

no set local-preference

Parameter	Parameter Description	Parameter Value
LOCAL-PREFERENCE	Species the preference value	0-4294967295

Command Mode

Route-map Configuration

Default

No set local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100
```

Related Commands

None

6.4.24 set metric

Command Purpose

Use this command to set a metric value for a route.

Use the no parameter with this command to disable this function.

This command sets the metric value for a route, and influences external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the `bgp always-compare-med` command.

To use the `set metric` command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set metric *METRICVAL*

no set metric

Parameter	Parameter Description	Parameter Value
METRICVAL	The metric value	0-4294967295

Command Mode

Route-map Configuration

Default

No set metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600
```

Related Commands

None

6.4.25 set metric-type

Command Purpose

Use this command to set the metric type for the destination routing protocol.

Use the no parameter with this command to return to the default.

This command sets the type to either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Command Syntax

set metric-type { type1 | type2 }

no set metric-type

Parameter	Parameter Description	Parameter Value
type1	Select to set external type 1 metric	-
type2	Select to set external type 2 metric	-

Command Mode

Route-map Configuration

Default

No set metric-type is specified by default.

Usage

This command is valid for OSPF only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1
```

Related Commands

None

6.4.26 set origin

Command Purpose

Use this command to set the BGP origin code.

Use the no parameter with this command to delete an entry.

The origin attribute defines the origin of the path information. The three parameters with this command indicate three different values. IGP is interior to the originating AS. This happens if IGP is redistributed into the BGP. EGP is learned through an Exterior Gateway Protocol. Incomplete is unknown or learned through some other means. This happens when static route is redistributed in BGP and the origin of the route is incomplete.

Command Syntax

```
set origin { egp | igp | incomplete }
```

```
no set origin
```

Parameter	Parameter Description	Parameter Value
egp	Specifies a remote EGP system	-
igp	A local IGP system	-
incomplete	Specifies a system of unknown heritage	-

Command Mode

Route-map Configuration

Default

No set origin is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

Related Commands

None

6.4.27 set originator-id

Command Purpose

Use this command to set the originator ID attribute.

Use the no parameter with this command to disable this function.

To use the set originator-id command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set originator-id *IPADDRESS*

no set originator-id

Parameter	Parameter Description	Parameter Value
IPADDRESS	Specifies the IP address of originator	IPv4 Address in A.B.C.D format

Command Mode

Route-map Configuration

Default

No set originator-id is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
```



```
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set originator-id 1.1.1.1
```

Related Commands

None

6.4.28 set tag

Command Purpose

Use this command to set a specified tag value.

Use the no parameter with this command to return to the default.

Tag in this command is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. Also, with using route-map, ZebOS can tag the LSAs with the appropriate tag value. Sometimes, the tag matches with using route-map, and sometimes, the value may be used by another application.

Command Syntax

set tag *TAGVALUE*

no set tag

Parameter	Parameter Description	Parameter Value
TAGVALUE	Tag value for destination routing protocol.	0-4294967295

Command Mode

Route-map Configuration

Default

No set tag is specified by default.

Usage

This command is valid for OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6
```

Related Commands

redistribute
default-information

6.4.29 set vpnv4 next-hop

Command Purpose

Use this command to set a VPNv4 next-hop address.
Use the no parameter with this command to disable this function

Command Syntax

set vpnv4 next-hop *IPADDRESS*
no set vpnv4 next-hop

Parameter	Parameter Description	Parameter Value
<i>IPADDRESS</i>	Specifies the IP address of next-hop	IPv4 Address in A.B.C.D format

Command Mode

Route-map Configuration

Default

No set vpnv4 next-hop is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv4 next-hop 6.6.6.6
```

Related Commands

None

6.4.30 set weight

Command Purpose

Use this command to set weights for the routing table.

Use the no parameter with this command to delete an entry.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

Command Syntax

set weight *WEIGHT*

no set weight

Parameter	Parameter Description	Parameter Value
WEIGHT	Specifies the weight value	0-4294967295

Command Mode

Route-map Configuration

Default

No set weight is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60
```

Related Commands

match as-path

6.4.31 show route-map

Command Purpose

Use this command to display user readable route-map information.

Command Syntax

show route-map (*NAME* |)

Parameter	Parameter Description	Parameter Value
NAME	route-map name	Up to 20 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch1# show route-map

route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
```

Related Commands

route-map

6.5 Prefix-list Commands

6.5.1 ip prefix-list

Command Purpose

To create a prefix list or add a prefix-list entry, use the `ip prefix-list` command in global configuration mode. To delete a prefix-list or an entry, use the `no` form of this command.

Command Syntax

```
ip prefix-list WORD ( seq SEQUENCE-NUMBER | ) ( deny | permit ) ( any | A.B.C.D/M ( ge GE-LENGTH | ) ( le LE-LENGTH | ) )
( any | A.B.C.D/M ( ge GE-LENGTH | ) ( le LE-LENGTH | ) )
no ip prefix-list WORD ( seq SEQUENCE-NUMBER | ) ( deny | permit ) ( any | A.B.C.D/M ( ge GE-LENGTH | ) ( le LE-LENGTH | ) )
no ip prefix-list WORD ( seq SEQUENCE-NUMBER | )
```

Parameter	Parameter Description	Parameter Value
WORD	Config a name to identify the prefix list	Up to 40 characters
seq SEQUENCE-NUMBER	Applies a sequence number to a prefix-list entry. If a sequence number is not entered when configuring this command, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5	1-65535
deny	Denies access for a matching condition	-
permit	Permits access for a matching condition	-
A.B.C.D/M	Configures the network address, and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32	IPv4 Address and mask length in A.B.C.D/M format
ge GE-LENGTH	(Optional)Specifies the lesser value of a range (the "from" portion of the range description) by applying the ge-length argument to the range specified. The ge-length argument represents the minimum prefix length to be matched	1-32
le LE-LENGTH	(Optional)Specifies the greater value of a range (the "to" portion of the range description) by applying the le-length argument to the range specified. The le-length argument represents the maximum prefix length to be matched	1-32

Command Mode

Global Configuration

Default

No prefix lists are created.

Usage

The ip prefix-list command is used to configure IP prefix filtering. Prefix lists are configured with permit or deny keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IP address and a bit mask. The IP address can be a classful network, a subnet, or a single host route. The bit mask is entered as a number from 1 to 32. An implicit deny is applied to traffic that does not match any prefix-list entry. Prefix lists are configured to match an exact prefix length or a prefix range. The ge and le keywords are used to specify a range of the prefix lengths to match, providing more flexible configuration than can be configured with just the network/length argument. The prefix list is processed using an exact match when neither the ge nor le keyword is entered. If only the ge

value is entered, the range is the value entered for the ge ge-length argument to a full 32-bit length. If only the le value is entered, the range is from value entered for the network/length argument to the le le-length argument. If both the ge ge-length and le le-length keywords and arguments are entered, the range falls between the values used for the ge-length and le-length arguments. The following formula shows this behavior:

Network/length < ge ge-length < le le-length <= 32.

A prefix list is configured with a name and/or sequence number. One or the other must be entered when configuring this command. If a sequence number is not entered, a default sequence number of 5 is applied to the prefix list. And subsequent prefix list entries will be increment by 5 (for example, 5, 10, 15, and onwards). If a sequence number is entered for the first prefix list entry but not subsequent entries, then the subsequent entries will also be incremented by 5 (For example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the no form of this command with the seq keyword. Prefix lists are evaluated starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the permit or deny statement is applied to that network and the rest of the list is not evaluated.

Examples

To deny the default route 0.0.0.0/0:

```
Switch# configure terminal
Switch(config)# ip prefix-list abc deny 0.0.0.0/0
```

To permit the prefix 10.0.0.0/8:

```
Switch# configure terminal
Switch(config)# ip prefix-list abc permit 10.0.0.0/8
```

To accept a mask length of up to 24 bits in routes with the prefix 192/16:

```
Switch# configure terminal
Switch(config)# ip prefix-list abc permit 192.168.0.0/16 le 24
```

To deny mask lengths greater than 25 bits in routes with the prefix 192/16:

```
Switch# configure terminal
Switch(config)# ip prefix-list abc deny 192.168.0.0/16 ge 25
```

Related Commands

- ip prefix-list description
- ip prefix-list sequence
- show ip prefix-list
- clear ip prefix-list

6.5.2 ip prefix-list description

Command Purpose

To add a text description of a prefix list, use the ip prefix-list description command in global configuration mode. To remove the text description, use the no form of this command

Command Syntax

ip prefix-list *WORD* description *LINE*

no ip prefix-list *WORD* description (*LINE*)

Parameter	Parameter Description	Parameter Value
WORD	Name of prefix list	Up to 40 characters
LINE	Up to 80 characters describing this prefix-list	Up to 80 characters

Command Mode

Global Configuration

Default

There is no description for prefix-list.

Usage

The prefix list will be created automatically if it didn't exist.

Examples

The following example shows how to add description:

```
Switch# configure terminal
Switch(config)# ip prefix-list abc description Deny routes from router A
```

Related Commands

```
ip prefix-list
ip prefix-list sequence
show ip prefix-list
clear ip prefix-list
```

6.5.3 ip prefix-list sequence-number

Command Purpose

To enable the generation of sequence numbers for entries in a prefix list, use the ip prefix-list sequence-number command in global configuration mode. To disable this function, use the no form of this command.

Command Syntax

ip prefix-list sequence-number

no ip prefix-list sequence-numbe

Command Mode

Global Configuration

Default

This command has no default behavior.

Usage

This command is used to enable sequence-number display.

Examples

The following example shows how to enable ip prefix-list sequence-number:

```
Switch# configure terminal
Switch(config)# ip prefix-list sequence-number
```

Related Commands

ip prefix-list

show ip prefix-list

clear ip prefix-list

6.5.4 show ip prefix-list

Command Purpose

To show prefix list information, use the show ip prefix-list command.

Command Syntax

show ip prefix-list (summary | detail |) (WORD |)

show ip prefix-list WORD (seq SEQUENCE-NUMBER | A.B.C.D/M (longer | first-match |) |)

Parameter	Parameter Description	Parameter Value
summary	Summary of prefix lists	-
detail	Detail of prefix lists	-
WORD	Name of the prefix list	Up to 40 characters
seq SEQUENCE-NUMBER	sequence number of the entry in the prefix list	1-65535
A.B.C.D/M	IP prefix <network>/<length>, e.g., 35.0.0.0/8	IPv4 Address and mask length in A.B.C.D/M format
longer	Lookup the mask of prefix longer than M	-
first-match	First matched prefix	-

Command Mode

Privileged EXEC

Default

This command has no default behavior.

Usage

None

Examples

The following example shows how to display ip prefix-list:

```
Switch# show ip prefix-list
```

```
ip prefix-list aa: 2 entries
```

```
    permit 1.1.1.0/24
```

```
    permit 1.2.3.0/24
```

Related Commands

ip prefix-list

clear ip prefix-list

6.5.5 clear ip prefix-list

Command Purpose

To Resets the hit count of the prefix list entries, use the clear ip prefix-list command.

Command Syntax

```
clear ip prefix-list ( WORD ( A.B.C.D/M | ) | )
```

Parameter	Parameter Description	Parameter Value
WORD	Name of the prefix list	Up to 40 characters
A.B.C.D/M	IP prefix <network>/<length>, e.g., 35.0.0.0/8	IPv4 Address and mask length in A.B.C.D/M format

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to clear ip prefix-list:

```
Switch# clear ip prefix-list abc
```

Related Commands

ip prefix-list

6.6 Policy-Based Routing Commands

6.6.1 ip policy route-map

Command Purpose

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR on a layer3 interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

Command Syntax

```
ip policy route-map MAP_NAME
```

```
no ip policy route-map
```

Parameter	Parameter Description	Parameter Value
<i>MAP_NAME</i>	policy route-map name	Up to 20 characters

Command Mode

Interface Configuration

Default

Disabled

Usage

This command can only be configured on routed port, vlan interface and routed agg port.

Examples

The following example shows how to configure pbr on an interface:

```
Switch# configure terminal
switch (config)# ip access-list 1 extend
switch (config-ex-ip-acl)# 10 permit any any any
switch (config-route-map)#exit
switch (config)#route-map richard permit 10
switch (config-route-map)#match ip address 1
switch (config-route-map)#set ip next-hop 10.1.1.1
switch (config-route-map)#exit
switch (config)#interface eth-0-1
switch (config-if)#no switch port
switch (config-if)#no shutdown
switch (config-if)#ip policy route-map richrad
```

Related Commands

route-map

6.6.2 show ip policy route-map

Command Purpose

Use this command to display user readable policy route-map information

Command Syntax

show ip policy route-map

Command Mode

Privileged EXEC

Default

Disabled

Usage

If some of the PBR entries are not successfully inserted into tcam, an error tip will be displayed.

Examples

```
SWITCH# show ip policy route-map
```

Route-map	interface
richard	eth-0-1
	eth-0-3

Failed entry: no

sally	eth-0-2

Failed entry: yes

Please use Policy Based-Routing CLI: show pbr failed entry to gain more detail.

Related Commands

route-map

6.6.3 show resource pbr

Command Purpose

Use this command to display the resource usage over the policy based routing module.

Command Syntax

show resource pbr

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

```
SWITCH# show resource pbr
```

Policy Based Routing

Resource	Used	Capability

```
=====
Policy Route Map          0          32
Policy Based Routing ACE  0          64
```

Related Commands

```
route-map
show ip policy route-map
```

6.7 BGP Commands

6.7.1 address-family

Command Purpose

Use this command to enter the IPv4, VPNv4 address-family command mode.

Command Syntax

```
address-family ipv4 ( unicast | vrf NAME | )
address-family vpnv4 ( unicast )
```

Parameter	Parameter Description	Parameter Value
vpnv4	Configures sessions for VPN-IPv4 prefixes. This parameter takes an IPv4 style address: A.B.C.D.	-
unicast	Specifies unicast prefixes	-
vrf	VPN routing/forwarding instance	-
NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Router Configuration

Default

None

Usage

Use the address family command to enter the address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the exit-address-family command.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
```

```
Switch(config-router)address-family ipv4
```

Related Commands

exit-address-family

Exit

6.7.2 aggregate-address

Command Purpose

Use this command to configure BGP aggregate entries.

Use the no parameter with this command to disable this function.

Command Syntax

(no) aggregate-address *IP_PREFIX* { summary-only | as-set }

Parameter	Parameter Description	Parameter Value
IP_PREFIX	A.B.C.D/M Specifies the aggregate prefix	IPv4 Address and mask length in A.B.C.D/M format
summary-only	Filters more specific routes from updates.	-
as-set	Generates AS set path information	-

Command Mode

Router Configuration

Default

Disabled

Usage

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. The aggregate-address command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the summary-only parameter advertises the prefix only, suppressing the more-specific routes to all neighbors.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# aggregate-address 10.0.0.0/8 as-set summary-only
```

Related Commands

N/A

6.7.3 bgp always-compare-med

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the no parameter with this command to disallow the comparison.

Command Syntax

(no) bgp always-compare-med

Command Mode

Router Configuration

Default

Disabled

Usage

Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

MED comparison is done only among paths from the same autonomous system (AS). Use bgp always-comparemed command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp always-compare-med
```

Related Commands

bgp bestpath med
bgp bestpath as-path ignore

6.7.4 bgp bestpath as-path ignore

Command Purpose

Use this command to prevent the router from considering as-path as a factor in the algorithm for choosing a route.

Use the no parameter with this command to allow the router to consider as-path in choosing a route.

Command Syntax

(no) bgp bestpath as-path ignore

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath as-path ignore
```

Related Commands

bgp always-compare-med, bgp bestpath med, bgp bestpath compare-routerid

6.7.5 bgp bestpath compare-confed-aspath

Command Purpose

Use this command to allow comparing of the confederation AS path length.

Use the no parameter with this command to revert the selection and ignore AS confederation path length in the BGP best path selection.

Command Syntax

(no) bgp bestpath compare-confed-aspath

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when `bgp bestpath as-path ignore` command has not been specified.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-confed-aspath
```

Related Commands

`bgp bestpath as-path ignore`

6.7.6 `bgp bestpath compare-routerid`

Command Purpose

Use this command to compare router-id for identical eBGP paths.
Use the `no` parameter with this command to disable this function.

Command Syntax

`( no ) bgp bestpath compare-routerid`

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

When comparing similar routes from peers the BGP router does not consider router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with lowest router ID is selected. The router-id is the highest IP address on the router, with preference given to loopback addresses. Router-id can be manually set by using the `bgp router-id` command.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-routerid
```

Related Commands

```
show ip bgp
show ip bgp neighbors
```

6.7.7 bgp bestpath med

Command Purpose

Use this command to specify Multi Exit Discriminator (MED) attribute comparison.

Use the `no` parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax

```
bgp bestpath med confed [ missing-as-worst ]
bgp bestpath med missing-as-worst [ confed ]
no bgp bestpath med confed [ missing-as-worst ]
no bgp bestpath med missing-as-worst [ confed ]
```

Parameter	Parameter Description	Parameter Value
confed	Compares MED among confederation paths	-
missing-as-worst	Treats missing MED as the least preferred one	-

Command Mode

Router Configuration

Default

MED value is zero.

Usage

Use this command to specify two MED attributes – confed and missing-as-worst. The confed attribute enables MED comparison among paths learned from confederation peers. The MEDs are compared only if there is no external autonomous system (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made.

The missing-as-worst attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If missing-as-worst is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath med missing-as-worst
```

Related Commands

bgp-always-compare-med, bgp bestpath as-path ignore, bgp deterministic-med

6.7.8 bgp client-to-client reflection

Command Purpose

Use this command to restore route reflection from a BGP route reflector to clients.

Use the no parameter with this command to turn off client-to-client reflection.

Command Syntax

bgp client-to-client reflection

no bgp client-to-client reflection

Parameter	Parameter Description	Parameter Value
reflection	Allows reflection of routes	-

Command Mode

Router Configuration

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Usage

The bgp client-to-client reflection command is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use no bgp client-to-client reflection command to disable the client-to-client route reflection.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) no bgp client-to-client reflection
```

Related Commands

bgp cluster-id
neighbor route-reflector-client
show ip bgp

6.7.9 bgp cluster-id

Command Purpose

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector.
Use the no parameter with this command to remove the cluster ID.

Command Syntax

bgp cluster-id *CLUSTERID*
no bgp cluster-id

Parameter	Parameter Description	Parameter Value
CLUSTERID	Specifies the cluster ID of this router acting as a route reflector, either as IP address or as a maximum of 4 bytes.	IPv4 Address in A.B.C.D format or number in range 1-4294967295
A.B.C.D	A.B.C.D Route Reflector Cluster-id in IP address format	IPv4 Address
1-4294967295	Route Reflector cluster-id as a 32 bit quantity	1-4294967295

Command Mode

Router Configuration

Default

N/A

Usage

A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The `bgp cluster-id` command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp cluster-id 1.1.1.1
```

Related Commands

`bgp client-to-client reflection`, `neighbor route-reflector-client`, `show ip bgp`

6.7.10 bgp confederation identifier

Command Purpose

Use this command to specify a Bgp confederation identifier.

Use the `no` parameter with this command to remove the Bgp confederation identifier.

Command Syntax

`bgp confederation identifier ID`

`no bgp confederation identifier`

Parameter	Parameter Description	Parameter Value
ID	Set routing domain confederation AS number	1-65535

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation identifier 1
```

Related Commands

bgp confederation peer

6.7.11 bgp confederation peers

Command Purpose

Use this command to configure the Autonomous Systems (AS) that belong to the confederation.

Use the no parameter with this command to remove an autonomous system from the confederation.

Command Syntax

```
bgp confederation peers .ASN
no bgp confederation peers ( .ASN | )
```

Parameter	Parameter Description	Parameter Value
ASN	AS numbers of eBGP peers that are under same confederation but in a different sub-AS	1-65535

Command Mode

Router Configuration

Default

N/A

Usage

A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation. Use the bgp confederation peer command to define the list of confederation peers.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation peers 1234 21345
```

Related Commands

bgp confederation identifier

6.7.12 bgp dampening

Command Purpose

Use this command to set bgp dampening parameters.

Use the no parameter with this command to unset the bgp dampening parameters.

Command Syntax

bgp dampening *REACHTIME*

bgp dampening *REACHTIME REUSE*

bgp dampening *REACHTIME REUSE SUPPRESS MAXSUPPRESS (UNREACHTIME |)*

bgp dampening route-map *ROUTEMAP*

no bgp dampening *REACHTIME*

no bgp dampening *REACHTIME REUSE*

no bgp dampening *REACHTIME REUSE SUPPRESS MAXSUPPRESS (UNREACHTIME |)*

no bgp dampening route-map (*ROUTEMAP* |)

Parameter	Parameter Description	Parameter Value
REACHTIME	Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes.	1-45
REUSE	Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750. <i>SUPPRESS <1-20000></i> Specifies the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000.	1-20000
SUPPRESS	Specifies suppress-time. A route dampening more than this value will be suppressed. The default value is 2000.	1-20000
MAXSUPPRESS	Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes).	1-255
UNREACHTIME	Specifies the un-reachability half-life time for penalty, in minutes.	1-45

Parameter	Parameter Description	Parameter Value
ROTEMAP	route-map WORD Route-map to specify criteria for dampening.	Up to 20 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is un-suppressed.

The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 800 2500 80 25
```

Related Commands

N/A

6.7.13 bgp default ipv4-unicast

Command Purpose

Use this command to configure BGP defaults and activate ipv4-unicast for a peer by default. This affects the BGP global configuration.

Use the no parameter with this command to disable this function

Command Syntax

```
bgp default ipv4-unicast
no bgp default ipv4-unicast
```

Command Mode

Router Configuration

Default

The bgp default ipv4 unicast is the default behavior.

Usage

The no bgp default ipv4-unicast command is used to disable the default behavior of the BGP routing process of exchanging IPv4 addressing information with BGP neighbor routers.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default ipv4-unicast
```

Related Commands

N/A

6.7.14 bgp default local-preference

Command Purpose

Use this command to change the default local preference value.

Use the no parameter with this command to revert to the default setting.

Command Syntax

```
bgp default local-preference PREF_VALUE
no default local-preference ( PREF_VALUE | )
```

Parameter	Parameter Description	Parameter Value
PREF_VALUE	Configure default local preference value. The default local preference value is 100.	0-4294967295

Command Mode

Router Configuration

Default

The default local preference value is 100.

Usage

Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. Use `bgp default local-preference` command to define preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default local-preference 2345555
```

Related Commands

N/A

6.7.15 `bgp deterministic-med`

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system.

Use the `no` parameter with this command to disallow this setting.

Command Syntax

```
bgp deterministic-med
no bgp deterministic-med
```

Command Mode

Router Configuration

Default

Disabled

Usage

"Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. Enable `bgp deterministic med` command on all routers in the local AS, for a correct comparison result. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value.

Based on this comparison, the best path is then chosen.

This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the `bgp always-compare-med` command."

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp deterministic-med
```

Related Commands

`show ip bgp`, `show ip bgp neighbors`

6.7.16 bgp enforce-first-as

Command Purpose

Use this command to specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied.

Use the `no` parameter with this command to disable this feature.

Command Syntax

```
bgp enforce-first-as
no bgp enforce-first-as
```

Command Mode

Router Configuration

Default

Disabled

Usage

Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp enforce-first-as
```

Related Commands

N/A

6.7.17 bgp fast-external-failover

Command Purpose

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down.
Use the no parameter with this command to disable this feature.

Command Syntax

```
bgp fast-external-failover  
no bgp fast-external-failover
```

Command Mode

Router Configuration

Default

Enabled

Usage

None

Examples

```
Switch# configure terminal  
Switch(config)# router bgp 100  
Switch(config-router)# bgp fast-external-failover
```

Related Commands

N/A

6.7.18 bgp log-neighbor-changes

Command Purpose

Use this command to enable logging of status change messages without turning on debug bgp commands.

Use the no parameter with this command to disable this feature.

Command Syntax

bgp log-neighbor-changes
no bgp log-neighbor-changes

Command Mode

Router Configuration

Default

Disabled

Usage

System implementation provides other kinds of logging services for neighbor status, for example, debug bgp fsm, debug bgp events, etc. However, these commands create a significant hit in the logging performance.

The bgp log-neighbor-changes command, logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp log-neighbor-changes
```

Related Commands

N/A

6.7.19 bgp router-id

Command Purpose

Use this command to configure the router identifier.

Use the no parameter with this command to disable this function

Command Syntax

bgp router-id *ROUTERID*

no bgp router-id (*ROUTERID* |)

Parameter	Parameter Description	Parameter Value
ROUTERID	A.B.C.D Manually configured router ID.	IPv4 Address in A.B.C.D format

Command Mode

Router Configuration

Address Family Configuration

Default

In case the loopback interface is configured the router-id is set to the IP address of a loopback interface. If not, the highest IP address is the router-id.

Usage

Use bgp router-id command to manually configure a fixed router ID as a BGP router identifier.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp router-id 1.1.2.3
```

Related Commands

N/A

6.7.20 bgp scan-time

Command Purpose

Use this command to set the interval for BGP route next-hop scanning.

Use the no parameter with this command to disable this function.

Command Syntax

bgp scan-time *TIME*

no bgp scan-time (*TIME* |)

Parameter	Parameter Description	Parameter Value
TIME	Scanning interval in seconds. The default scanning interval is 60 seconds.	0-60

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database.

To disable BGP scanning, set the scan time interval to 0 seconds.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp scan-time 10
```

Related Commands

N/A

6.7.21 clear ip bgp *

Command Purpose

Use this command to reset a BGP connection for all peers.

Command Syntax

clear ip bgp * (*IN* | out | *SOFT* |)

clear ip bgp * ipv4 *PREFIX ROUTES*

clear ip bgp * vpnv4 unicast *ROUTES*

clear ip bgp * vrf *NAME ROUTES*

Parameter	Parameter Description	Parameter Value
*	clears all bgp peers	-
ipv4	clears all IPv4 address family peers	-
vpnv4	clears all vpnv4 address family peers	-
ROUTES	(IN out SOFT)	-
IN	in (prefix-filter)	-
in	Indicates that incoming advertised routes will be cleared	-
prefix-filter	Pushes out prefix-list ORF and does inbound soft reconfiguration	-
out	Indicates that outgoing advertised routes will be cleared.	-
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-
vrf	VPN routing/forwarding instance	-
NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

There are two kinds BGP reset, hard reset will clear BGP peers and establish again. Soft reset only refresh routing table.

Examples

```
Switch# clear ip bgp *
Switch# clear ip bgp * ipv4 unicast in prefix-filter
Switch# clear ip bgp * vpnv4 unicast in
```

Related Commands

N/A

6.7.22 clear ip bgp A.B.C.D

Command Purpose

Use this command to reset a IPv4 BGP connection for a specific IP address.

Command Syntax

clear ip bgp *A.B.C.D* (in | out | *SOFT*)

clear ip bgp *A.B.C.D* ipv4 *PREFIX ROUTES*

clear ip bgp *A.B.C.D* vpnv4 unicast *ROUTES*

clear ip bgp *A.B.C.D* vrf *NAME ROUTES*

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IPv4 address of the BGP route to be cleared	IPv4 Address in A.B.C.D format
ipv4	clears all IPv4 address family peers	-
vpnv4	clears all VPNv4 address family peers	-
ROUTES	(IN out SOFT)	-
IN	in prefix-filter	-
in	Indicates that incoming advertised routes will be cleared	-
prefix-filter	Pushes out prefix-list ORF and does inbound soft reconfiguration	-
out	Indicates that outgoing advertised routes will be cleared.	-
Parameter	Parameter Description	Parameter Value
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-
vrf	VPN routing/forwarding instance	-
NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear ip bgp 10.10.0.12 soft
Switch# clear ip bgp 10.10.0.10 vpv4 unicast out
Switch# clear ip bgp 11.11.11.11 ipv4 multicast in prefix-filter
```

Related Commands

N/A

6.7.23 clear ip bgp dampening

Command Purpose

Use this command to reset all dampened BGP routes under the specified address family.

Command Syntax

clear ip bgp dampening (*A.B.C.D* | *A.B.C.D/M* |)

clear ip bgp ipv4 *PREFIX* dampening (*A.B.C.D* | *A.B.C.D/M* |)

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IPv4 address for which Bgp dampening is to be cleared.	IPv4 Address in A.B.C.D format
A.B.C.D/M	Specifies the IPv4 address with mask for which Bgp dampening is to be cleared.	IPv4 Address and mask length in A.B.C.D/M format
ipv4	clears all IPv4 address family peers	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear ip bgp dampening 10.10.0.121
```

```
Switch# clear ip bgp ipv4 unicast dampening
```

Related Commands

N/A

6.7.24 clear ip bgp flap-statistics

Command Purpose

Use this command to clear the flap count and history duration for all the prefixes under the specified address family.

Command Syntax

clear ip bgp flap-statistics (*A.B.C.D* | *A.B.C.D/M* |)

clear ip bgp ipv4 *PREFIX* flap-statistics (*A.B.C.D* | *A.B.C.D/M* |)

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IPv4 address for which Bgp dampening is to be cleared.	IPv4 Address in A.B.C.D format
A.B.C.D/M	Specifies the IPv4 address with mask for which Bgp dampening is to be cleared.	IPv4 Address and mask length in A.B.C.D/M format
ipv4	clears all IPv4 address family peers	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear ip bgp flap-statistics 10.10.0.121
```

```
Switch# clear ip bgp ipv4 unicast flap-statistics
```

Related Commands

N/A

6.7.25 clear ip bgp ASN

Command Purpose

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax

```
clear ip bgp ASN ( IN | out | SOFT | )
```

```
clear ip bgp ASN ipv4 PREFIX ROUTES
```

```
clear ip bgp ASN vpnv4 unicast ROUTES
```

Parameter	Parameter Description	Parameter Value
ASN	Specifies the AS Number for which all routes will be cleared	1-65535
ipv4	clears all IPv4 address family peers	-
vpnv4	clears all VPNv4 address family peers	-
ROUTES	(IN out SOFT)	-
IN	in prefix-filter	-
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
prefix-filter	Pushes out prefix-list ORF and does inbound soft reconfiguration	-
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear ip bgp 100
Switch# clear ip bgp 200 ipv4 unicast in prefix-filter
Switch# clear ip bgp 500 vpnv4 unicast in
```

Related Commands

N/A

6.7.26 clear ip bgp external**Command Purpose**

Use this command to reset a BGP connection for all external peers.

Command Syntax

```
clear ip bgp external ( In | out | SOFT | )
```

```
clear ip bgp external ipv4 PREFIX ROUTES
```

Parameter	Parameter Description	Parameter Value
external	Clears all external peers	-
ROUTES	(IN out SOFT)	-
IN	in prefix-filter	-
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
ipv4	clears all IPv4 address family peers	-

Parameter	Parameter Description	Parameter Value
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear ip bgp external out
Switch# clear ip bgp external ipv4 unicast in prefix-filter
```

Related Commands

N/A

6.7.27 clear ip bgp peer-group

Command Purpose

Use this command to reset a BGP connection for all members of a peer group.

Command Syntax

```
clear ip bgp peer-group WORD ( In | out | SOFT | )
```

```
clear ip bgp peer-group WORD ipv4 PREFIX ROUTES
```

Parameter	Parameter Description	Parameter Value
peer-group	Clears all members of a peer group	-
WORD	Specifies the name of the peer group for which all members will be cleared.	Up to 20 characters
ipv4	clears all IPv4 address family peers	-
ROUTES	(IN out SOFT)	-
prefix-filter	Pushes out prefix-list ORF and does inbound soft reconfiguration	-

Parameter	Parameter Description	Parameter Value
IN	in prefix-filter	-
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
PREFIX	(unicast multicast)	-
unicast	address family modifier	-
multicast	address family modifier	-

Command Mode

Privileged EXEC

Default

N/A

Usage

None

Examples

```
Switch# clear ip bgp peer-group Peer1 out
Switch# clear ip bgp peer-group mypeer ipv4 unicast in prefix-filter
```

Related Commands

N/A

6.7.28 clear ip bgp vrf

Command Purpose

Use this command to reset the specified VPN Routing /Forwarding Instance for BGP connections.

Command Syntax

```
clear ip bgp ( A.B.C.D ) | * ) vrf WORD ( out | in | SOFT )
```

Parameter	Parameter Description	Parameter Value
WORD	Specifies the name of the VRF	Up to 15 characters

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the IPv4 address of the BGP route to be cleared	IPv4 Address in A.B.C.D format
*	Clears all peers	-
out	Performs soft reconfiguration out	-
SOFT	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
in	Performs soft reconfiguration in	-

Command Mode

Privileged EXEC

Default

N/A

Usage

If the neighbor address is specified with this command it clears the specified connection. If no address is specified this command clears all the BGP routes.

Examples

```
Switch# clear ip bgp 3.3.3.3 vrf VRF1 soft in
```

Related Commands

N/A

6.7.29 debug bgp

Command Purpose

Use this command to specify all debugging options for BGP. Use the no parameter with this command to disable this function.

Command Syntax

debug bgp (all | dampening | events | filters | fsm | keepalives | mpls | updates)

no debug bgp (all | dampening | events | filters | fsm | keepalives | mpls | nsm | updates)

Parameter	Parameter Description	Parameter Value
all	Used with the no form exclusively; turns off all debugging for BGP	-
dampening	Specifies debugging for Bgp dampening.	-

Parameter	Parameter Description	Parameter Value
events	Specifies debugging for BGP events.	-
filters	Specifies debugging for BGP filters.	-
fsm	Specifies debugging for BGP Finite State Machine (FSM).	-
mpls	Specifies debuggin for BGP Multiprotocol Label Switching.	-
keepalives	Specifies debugging for BGP keepalives.	-
updates	updates Specifies debugging for BGP updates.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

This command without any parameters turns on normal bgp debug information.

Examples

```
Switch# debug bgp
Switch# debug bgp events
```

Related Commands

N/A

6.7.30 distance

Command Purpose

Use this command to define an administrative distance.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

```
distance ADMINDISTANCE IP_ADDR/IP_MASK_LEN
no distance ADMINDISTANCE IP_ADDR/IP_MASK_LEN
```

Parameter	Parameter Description	Parameter Value
ADMINDISTANCE	Specifies the administrative distance.	1-255
IP_ADDR	the IP source prefix	IPv4 Address
IP_MASK_LEN	the IP source prefix mask length	1-32

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to set the administrative distance for BGP. This distance is a rating of trustworthiness of a router.

The higher the distance the lower the trust rating.

The administrative distance can be set for external, internal and local routes. External paths are routes learned from a neighbor out of the AS. The internal routes are routes learned from another router within the same AS. Local routes are for the router that is being redistributed from another process.

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance 34 10.10.0.0/24 mylist
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) distance bgp 34 23 15
```

Related Commands

N/A

6.7.31 exit-address-family

Command Purpose

Use this command to exit the address family mode.

Command Syntax

exit-address-family

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example shows the use of exit-address-family command and the change in the prompt after using this command:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

Related Commands

address-family

6.7.32 ip as-path access-list

Command Purpose

Use this command to define a BGP Autonomous System (AS) path access list.

Use the no parameter with this command to disable use of the access list.

Command Syntax

ip as-path access-list *LISTNAME* (deny | permit) *LINE*

no ip as-path access-list *LISTNAME* (deny | permit) *LINE*

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the name of the access list.	Up to 40 characters, the first character must be among [a-zA-Z0-9]
deny	(Optional) Denies access to matching conditions.	-
permit	(Optional) Permits access to matching conditions.	-

Parameter	Parameter Description	Parameter Value
LINE	Specifies a regular expression to match the BGP AS paths.	A regular expression to match the BGP AS paths

Command Mode

Global Configuration

Default

N/A

Usage

Named community list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the permit or deny condition applies. Use this command to define the BGP access list globally, use the neighbor router configuration command to apply a specific access list.

Examples

```
Switch# configure terminal
Switch(config)# ip as-path access-list mylist deny ^65535$
```

Related Commands

N/A

6.7.33 ip community-list

Command Purpose

Use this command to add a community list entry.

Use the no parameter with this command to delete the community list entry.

Command Syntax

ip community-list *LISTNUM* (deny | permit) *COMMUNITY*

no ip community-list *LISTNUM* (deny | permit) *COMMUNITY*

Parameter	Parameter Description	Parameter Value
LISTNUM	Specifies the community ID. 1-99:Standard list 100-199:Expands list	1-199
deny	Specifies the community to reject.	-
permit	Specifies the community to accept.	-

Parameter	Parameter Description	Parameter Value
COMMUNITY	(AA:NN internet local-AS no-advertise no-export)	-
AA:NN	Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.	AA is in the range 1-65535 NN is in the range of 1-65535
internet	Specifies routes not to be advertised to the Internet.	-
local-AS	Specifies routes not to be advertised to external BGP peers.	-
no-advertise	Specifies routes not to be advertised to other BGP peers.	-
no-export	Specifies routes not to be advertised outside of Autonomous System boundary.	-

Command Mode

Global Configuration

Default

N/A

Usage

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.

There are two kinds of community-lists: the expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Examples

```
Switch# configure terminal
Switch(config)# ip community-list 20 permit 7675:80 7675:90
```

Related Commands

ip community-list standard
ip community-list expanded

6.7.34 ip community-list expanded

Command Purpose

Use this command to add a community list entry.

Use the no parameter with this command to delete the community list entry.

Command Syntax

ip community-list expanded *WORD* (deny | permit) *LINE*

no ip community-list expanded *WORD* (deny | permit) *LINE*

Parameter	Parameter Description	Parameter Value
expanded	Add an expanded community-list entry.	-
WORD	Expanded community list name	Up to 20 characters
deny	Specifies community to reject.	-
permit	Specifies community to accept.	-
LINE	Specifies a regular expression to match the BGP AS paths.	A regular expression

Command Mode

Global Configuration

Default

N/A

Usage

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.

There are two kinds of community-lists – the expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Examples

```
Switch# configure terminal
Switch(config)# ip community-list expanded CLIST permit .*
```

Related Commands

ip community-list

ip community-list standard

6.7.35 ip community-list standard

Command Purpose

Use this command to add a standard community-list entry.

Use the no parameter with this command to delete the standard community-list entry.

Command Syntax

ip community-list standard *WORD* (deny | permit) *COMMUNITY*

no ip community-list standard *WORD* (deny | permit) *COMMUNITY*

Parameter	Parameter Description	Parameter Value
standard	Specifies a standard community list.	-
WORD	Standard community list name	Up to 20 characters
deny	Specifies community to reject.	-
permit	Specifies community to accept.	-
COMMUNITY	(AA:NN internet local-AS no-advertise no-export)	-
AA: NN	Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.	AA is in the range 1-65535 NN is in the range of 1-65535
internet	Specifies routes not to be advertised to the Internet.	-
local-AS	Specifies routes not to be advertised to external BGP peers.	-
no-advertise	Specifies routes not to be advertised to other BGP peers.	-
no-export	Specifies routes not to be advertised outside of the Autonomous System boundary.	-

Command Mode

Global Configuration

Default

N/A

Usage

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long.

There are two kinds of community-lists – the expanded and standard. The standard community-list defines the community attributes in a specified format without regular expressions. The expanded community-list defines the communities attributes with regular expressions.

Use the `ip community-list standard` command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Examples

```
Switch# configure terminal
Switch(config)# ip community-list standard CLIST permit 7675:80 7675:90 no-export
```

Related Commands

`ip community-list`
`ip community-list expanded`

6.7.36 neighbor activate

Command Purpose

Use this command to enable the exchange of the specified AF routes with a neighboring router.
 Use the `no` parameter with this command to disable exchange of information with a neighbor.

Command Syntax

`neighbor NEIGHBORID activate`
`no neighbor NEIGHBORID activate`

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the <code>neighbor peer-group</code> and <code>neighbor remote-as</code> commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

After the TCP connection is opened with the neighbor, this command is used to enable or disable the exchange of the specified AF information with a neighboring router.

To enable the exchange of multicast and VPNv4 address prefix types, neighbors are activated using the neighbor activate command in address family mode.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 activate
```

Related Commands

neighbor remote-as

6.7.37 neighbor advertisement-interval

Command Purpose

Use this command to set the minimum interval between sending the BGP routing updates.

Use the no parameter with this command to set the interval time to default.

Command Syntax

neighbor *NEIGHBORID* advertisement-interval *TIME*

no neighbor *NEIGHBORID* advertisement-interval *TIME*

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
TIME	Advertise -interval value in seconds	0-600

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to set the minimum interval between the sending of BGP routing updates. To reduce the flapping of routes to internet, a minimum advertisement interval is set, so that the BGP routing updates are sent only per interval seconds. bgp dampening can also be used to control the effects of flapping routes. For the originated bgp routes, they would be sent out when as-origination-interval and advertisement-interval expired at the same time.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.3 advertisement-interval 45
```

Related Commands

N/A

6.7.38 neighbor as-origination-interval

Command Purpose

Use this command to set the minimum interval between ready to send the originated BGP routing updates.
Use the no parameter with this command to set the interval time to default.

Command Syntax

```
neighbor NEIGHBORID as-origination-interval TIME
no neighbor NEIGHBORID as-origination-interval TIME
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D)[TAG]	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
TIME	Advertise -interval value in seconds	0-600

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to set the minimum interval between the ready to send of originated BGP routing updates. For the originated bgp routes, they would be sent out when as-origination-interval and advertisement-interval expired at the same time.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.3 advertisement-interval 45
```

Related Commands

N/A

6.7.39 neighbor allowas-in

Command Purpose

Use this command to configure PE routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs).

Use the no parameter with this command to disable the readvertisement of a PE router's ASN.

Command Syntax

neighbor *NEIGHBOR* allowas-in [*NUMBER*]

no neighbor *NEIGHBOR* allowas-in

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
NUMBER	Number of occurrences of AS number. Default value is 1	1-10

Command Mode

Router Configuration

Address Family Configuration

Default

Disabled

Usage

In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Use the neighbor allowas-in command to configure two VRFs on each PE router to receive and re-advertise prefixes. One of the VRFs receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with ASNs from the CE router and re-advertises them to all PE routers in the hub and spoke configuration.

Control the number of times an ASN is advertised, by specifying a number from 1 to 10.

Examples

```
Switch# configure terminal
Switch(config-router)# address-family ipv4 vrf VRF_A
Switch(config-router-af)# neighbor 10.10.0.1 allowas-in 3
```

Related Commands

N/A

6.7.40 neighbor attribute-unchanged

Command Purpose

Use this command to advertise unchanged BGP attributes to the specified neighbor.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* attribute-unchanged { as-path | next-hop | med }

no neighbor *NEIGHBORID* attribute-unchanged { as-path | next-hop | med }

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
as-path	AS path attribute	-
next-hop	Next hop attribute	-
med	Multi Exit Discriminator	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.75 attribute-unchanged as-path med
```

Related Commands

N/A

6.7.41 neighbor capability dynamic

Command Purpose

Use this command to enable the dynamic capability for a specific peer.

Use the no parameter with this command to disable the dynamic capability.

Command Syntax

neighbor *NEIGHBORID* capability dynamic

no neighbor *NEIGHBORID* capability dynamic

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

Disabled

Usage

This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability dynamic
```

Related Commands

N/A

6.7.42 neighbor capability orf prefix-list

Command Purpose

Use this command to advertise ORF capability to neighbors.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* capability orf prefix-list (both | receive | send)

no neighbor *NEIGHBORID* capability orf prefix-list (both | receive | send)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
orf	Advertises ORF capability to its neighbors	-
both	Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.	-
receive	Indicates that the local router is willing to receive ORF entries from its peer	-
send	Indicates that the local router is willing to send ORF entries to its peer	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The local router advertises the ORF capability in send mode and the remote router receives the ORF capability in receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.1.1.1 capability orf prefix-list both
```

Related Commands

N/A

6.7.43 neighbor capability route-refresh

Command Purpose

Use this command to advertise route-refresh capability to the specified neighbors.

Use the no parameter with this command to disable this function

Command Syntax

neighbor *NEIGHBORID* capability route-refresh

no neighbor *NEIGHBORID* capability route-refresh

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to advertise to peer about route refresh capability support. If route refresh capability is supported, then router can dynamically request that the peer readvertises its Adj-RIB-Out.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 capability route-refresh
```

Related Commands

N/A

6.7.44 neighbor default-originate

Command Purpose

Use this command to allow a BGP local router to send the default route 0.0.0.0 to a neighbor for use as a default route.
Use the no parameter with this command to send no route as a default.

Command Syntax

neighbor *NEIGHBORID* default-originate (*ROUTEMAP* |)

no neighbor *NEIGHBORID* default-originate (*ROUTEMAP* |)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
ROUTEMAP	route-map WORD	-
route-map	The route-map to specify criteria to originate default routes	-
WORD	Route-map name	Up to 20 characters

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

Every router should have a default route, it is used to send datas to the network which is not existent in local RIB. To set a default route on each router can make every router have a default route, or to create a default route and broadcast it to BGP peer by this command.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.1 default-originate route-map myroute
```

Related Commands

N/A

6.7.45 neighbor description

Command Purpose

Use this command to associate a description with a neighbor.

Use the no parameter with this command to remove the description.

Command Syntax

neighbor *NEIGHBORID* description *LINE*

no neighbor *NEIGHBORID* description

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
LINE	A string to describing the neighbor.	Up to 80 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 description Backup router for sales.
```

Related Commands

N/A

6.7.46 neighbor distribute-list**Command Purpose**

Use this command to filter route update from a particular BGP neighbor.

Use the no parameter with this command to remove an entry.

Command Syntax

neighbor *NEIGHBORID* distribute-list *WORD* (in | out)

no neighbor *NEIGHBORID* distribute-list *WORD* (in | out)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
WORD	The name of IP access-list	Up to 40 characters
in	Indicates that incoming advertised routes will be filtered.	-
out	Indicates that outgoing advertised routes will be filtered.	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

Use only one distribute-list per BGP neighbor.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 1.2.3.4 distribute-list mylist out
```

Related Commands

N/A

6.7.47 neighbor ebgp-multihop**Command Purpose**

Use this command to accept and attempt BGP connections to external peers on indirectly connected networks.

Use the no parameter with this command to return to the default.

Command Syntax

neighbor *NEIGHBORID* ebgp-multihop (*COUNT* |)

no neighbor *NEIGHBORID* ebgp-multihop

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
COUNT	Maximum hop count. If the maximum hop count is not set the hop count is 255.	1-255

Command Mode

Router Configuration

Default

N/A

Usage

Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.10.34 remote-as 20
Switch(config-router)# neighbor 10.10.10.34 ebgp-multihop 5
```

Related Commands

N/A

6.7.48 neighbor filter-list**Command Purpose**

Use this command to set up a BGP filter.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* filter-list *LISTNAME* (in | out)

no neighbor *NEIGHBORID* filter-list *LISTNAME* (in | out)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
in	Indicates that incoming advertised routes will be filtered.	-
out	Indicates that outgoing advertised routes will be filtered.	-

Parameter	Parameter Description	Parameter Value
LISTNAME	The name of an autonomous system path access list.	Up to 40 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.34 filter-list listname out
```

Related Commands

N/A

6.7.49 neighbor maximum-prefix

Command Purpose

Use this command to control the number of prefixes that can be received from a neighbor.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* maximum-prefix *MAXIMUM*

no neighbor *NEIGHBORID* maximum-prefix

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
MAXIMUM	MAXPREFIX (THRESHOLD) (warning-only)	-
MAXPREFIX	Specifies the maximum number of prefixes permitted.	1-4294967295
THRESHOLD	<1-100> Specifies the threshold value, 1 to 100 percent.	1-100
warning-only	Only gives a warning message when the limit is exceeded.	-

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

The neighbor maximum-prefix command allows the configuration of a specified number of prefixes that a BGP router is allowed to receive from a neighbor. When the warning-only option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the clear ip bgp command is used.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 maximum-prefix 1244 warning-only
```

Related Commands

N/A

6.7.50 neighbor next-hop-self

Command Purpose

Use this command to configure the router as the next hop for a BGP-speaking neighbor or peer group.
Use the no parameter with this command to disable this feature.

Command Syntax

neighbor *NEIGHBORID* next-hop-self

no neighbor *NEIGHBORID* next-hop-self

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D)[TAG]	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 remote-as 100
Switch(config-router)# neighbor 10.10.0.72 next-hop-self
```

Related Commands

N/A

6.7.51 neighbor override-capability

Command Purpose

Use this command to override a capability negotiation result.

Use the no parameter with this command to disable this function

Command Syntax

neighbor *NEIGHBORID* override-capability

no neighbor *NEIGHBORID* override-capability

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 override-capability
```

Related Commands

N/A

6.7.52 neighbor passive

Command Purpose

Use this command to set a BGP neighbor as passive.

Use the no parameter with this command to disable this function

Command Syntax

(no) neighbor NEIGHBORID passive

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 passive
```

Related Commands

N/A

6.7.53 neighbor peer-group (adding a neighbor)

Command Purpose

Use this command to add a neighbor to an existing peer-group.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *IPADDRESS* peer-group *TAG*

no neighbor *IPADDRESS* peer-group

Parameter	Parameter Description	Parameter Value
IPADDRESS	A.B.C.D Specifies the address of the BGP neighbor in IPv4 format. A.B.C.D Specifies the address of the BGP neighbor in IPv4 format. TAG Name of the peer-group	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the neighbor peer-group create command and then use this command to add neighbors to the group.

Examples

This example shows a new peer-group group1 and the adding of a neighbor 10.10.0.63 to the group:

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
Switch(config-router)# neighbor 10.10.0.63 peer-group group1
```

Related Commands

N/A

6.7.54 neighbor peer-group (creating a peer-group)

Command Purpose

Use this command to create a peer-group.

Use the no parameter with this command to disable this function

Command Syntax

neighbor TAG peer-group

no neighbor TAG peer-group

Parameter	Parameter Description	Parameter Value
TAG	Name of the peer-group	-

Command Mode

Router Configuration

Default

N/A

Usage

Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
```

Related Commands

N/A

6.7.55 neighbor prefix-list

Command Purpose

Use this command to distribute BGP neighbor information as specified in a prefix list.

Use the no parameter with this command to remove an entry.

Command Syntax

neighbor *NEIGHBORID* prefix-list *LISTNAME* (in | out)

no neighbor *NEIGHBORID* prefix-list *LISTNAME* (in | out)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
LISTNAME	The number of an AS-path access list.	Up to 40 characters
in	Specifies that the access list applies to incoming advertisements.	-
out	Specifies that the access list applies to outgoing advertisements.	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

Use this command to specify a prefix list for filtering BGP advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top.

The neighbor distribute-list command is an alternative to the neighbor prefix-list command and only

one of them can be used for filtering to the same neighbor in any direction.

Examples

```
Switch# configure terminal
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 prefix-list list1 in
```

Related Commands

ip prefix-list

6.7.56 neighbor remote-as

Command Purpose

Use this command to configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

Command Syntax

neighbor *NEIGHBORID* remote-as *ASNUM*

no neighbor *NEIGHBORID* remote-as *ASNUM*

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
ASNUM	Neighbor's autonomous system number	1-4294967295

Command Mode

Router Configuration

Default

N/A

Usage

This command is used to configure iBGP and eBGP sessions with other neighbors. A peer-group support of this command is configured only after creating a specific peer-group.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# neighbor 10.10.0.73 remote-as 345
```

Related Commands

N/A

6.7.57 neighbor remove-private-AS

Command Purpose

Use this command to remove the private Autonomous System (AS) number from outbound updates.

Use the no parameter with this command too revert to default.

Command Syntax

neighbor *NEIGHBORID* remove-private-AS

no neighbor *NEIGHBORID* remove-private-AS

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Address Family Configuration

Default

Disabled

Usage

The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.63 remove-private-AS
```

Related Commands

N/A

6.7.58 neighbor route-reflector-client

Command Purpose

Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client.

Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax

neighbor *NEIGHBORID* route-reflector-client

no neighbor *NEIGHBORID* route-reflector-client

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the `neighbor route-reflector-client` command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 route-reflector-client
```

Related Commands

N/A

6.7.59 neighbor send-community

Command Purpose

Use this command to specify that a community attribute should be sent to a BGP neighbor.

Use the `no` parameter with this command to remove the entry. Use the `extended` and `no` parameters to remove extended communities. Specifying no other parameter means standard communities only.

Command Syntax

`neighbor NEIGHBORID send-community ( both | extended | standard | )`

`no neighbor NEIGHBORID send-community ( both | extended | standard | )`

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the <code>neighbor peer-group</code> and <code>neighbor remote-as</code> commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Parameter	Parameter Description	Parameter Value
both	Sends Standard and Extended Community attributes	-
extended	Sends Extended Community attributes	-
standard	Sends Standard Community attributes	-

Command Mode

Router Configuration

Address Family Configuration

Default

None

Usage

By default ,community attributes are not sent to a neighbor.To use this command to enable this command.Route-map can be based on neighbor address, peer group name or AS path information.

Examples

```
Switch# configure terminal
Switch(config)# bgp config-type standard
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 send-community extended
```

Related Commands

N/A

6.7.60 neighbor shutdown

Command Purpose

Use this command to disable a neighbor.

Use the no parameter with this command to re-enable the neighbor.

Command Syntax

neighbor *NEIGHBORID* shutdown

no neighbor *NEIGHBORID* shutdown

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

This command shuts down any active session for the specified neighbor and clears all related routing data.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 shutdown
```

Related Commands

N/A

6.7.61 neighbor soft-reconfiguration inbound

Command Purpose

Use this command to configure to start storing updates.

Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor NEIGHBORID soft-reconfiguration inbound
no neighbor NEIGHBORID soft-reconfiguration inbound
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 soft-reconfiguration inbound
```

Related Commands

N/A

6.7.62 neighbor strict-capability-match

Command Purpose

Use this command to close the BGP connection if capability value does not completely match to remote peer.
Use the no parameter with this command to disable this function

Command Syntax

neighbor *NEIGHBORID* strict-capability-match

no neighbor *NEIGHBORID* strict-capability-match

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 strict-capability-match
```

Related Commands

N/A

6.7.63 neighbor timers

Command Purpose

Use this command to set the timers for a specific BGP neighbor.

Use the no parameter with this command to clear the timers for a specific BGP neighbor

Command Syntax

neighbor *NEIGHBORID* timers *KEEPALIVE HOLDTIME*

no neighbor *NEIGHBORID* timers

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D)[TAG]	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
KEEPALIVE	holdtime Frequency (in seconds) at which a router sends keepalive messages to its neighbor. The default is 60 seconds.	1-65535
HOLDTIME	Interval (in seconds) after which, on not receiving a keepalive message, the router declares a neighbor dead. The default is 180 seconds.	3-65535

Command Mode

Router Configuration

Default

N/A

Usage

Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive a message for this period it declares the neighbor dead.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 timers 60 120
```

Related Commands

N/A

6.7.64 neighbor unsuppress-map

Command Purpose

Use this command to selectively leak more-specific routes to a particular neighbor.

Command Syntax

neighbor *NEIGHBORID* unsuppress-map *WORD*

no neighbor *NEIGHBORID* unsuppress-map *WORD*

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
WORD	Name of route map	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

When the aggregate-address command is used with the summary-only option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the unsuppress-map command to selectively leak more-specific routes to a particular neighbor.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router) neighbor 10.10.0.73 unsuppress-map mymap
Switch#configure terminal
Switch(config)#router bgp 10
Switch(config-router)address-family ipv4 unicast
```

```
Switch(config-router-af)neighbor 10.10.0.70 unsuppress-map mymap
```

Related Commands

N/A

6.7.65 neighbor update-source

Command Purpose

Use this command to allow internal BGP sessions to use any operational interface for TCP connections.

Use the no parameter with this command to restore the interface assignment to the closest interface.

Command Syntax

neighbor NEIGHBORID update-source IFNAME

no neighbor NEIGHBORID update-source

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
IFNAME	Specifies the loopback interface.	Support physical/aggregation/loopback/tunnel/vlan interfaces

Command Mode

Router Configuration

Default

N/A

Usage

Use this command in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 10.10.0.72 update-source eth-0/1
```

Related Commands

N/A

6.7.66 neighbor weight

Command Purpose

Use this command to set default weights for routes from this neighbor.
Use the no parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor NEIGHBORID weight WEIGHT
no neighbor NEIGHBORID weight
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(A.B.C.D TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
WEIGHT	Specifies the weight this command assigns to the route.	0-65535

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to specify a weight value to all routes learned from a neighbor. The route with the highest weight gets preference when there are other routes on the network.

Unlike the local-preference attribute, the weight attribute is relevant only to the local router.

The weights assigned using the set weight command overrides the weights assigned using this command.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 weight 60
```

Related Commands

N/A

6.7.67 neighbor fall-over bfd

Command Purpose

Use this command to establish BFD session on BGP neighbour.

Use the no parameter with this command to delete BFD session on BGP neighbour.

Command Syntax

```
neighbor A.B.C.D fall-over bfd
no neighbor A.B.C.D fall-over bfd
```

Parameter	Parameter Description	Parameter Value
A.B.C.D	Specifies the address of the BGP neighbor in IPv4 format.	IPv4 Address in A.B.C.D format

Command Mode

Router Configuration

Default

N/A

Usage

Enabling bfd on bgp neighbor.

Examples

```
Switch# configure terminal
```

```
Switch(config)# router bgp 12
Switch(config-router)# neighbor 10.10.10.10 fall-over bfd
```

Related Commands

6.7.68 network

Command Purpose

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the no form of this command to remove a network route entry.

Command Syntax

network *A.B.C.D*

network *A.B.C.D* route-map *WORD*

no network *A.B.C.D*

no network *A.B.C.D* route-map *WORD*

Parameter	Parameter Description	Parameter Value
A.B.C.D	IP prefix <network>, e.g., 35.0.0.0	IPv4 Address in A.B.C.D format
WORD	Name of the route map	Up to 20 characters

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 will be internally derived, that is, 2.0.0.0/8:

```
Switch# configure terminal
Switch(config)#router bgp 1
Switch(config-router)#network 2.0.0.0
```

```
!  
router bgp 1  
no synchronization  
network 2.0.0.0  
!
```

Related Commands

N/A

6.7.69 network synchronization

Command Purpose

Use this command to ensure the exact same static network prefix, specified through any of the network commands, is local or has IGP reachability (in the NSM RIB) before being introduced into the BGP RIB.

Use the no parameter with this command to disable this function.

Command Syntax

```
network synchronization  
no network synchronization
```

Command Mode

Router Configuration
Address Family Configuration

Default

Network synchronization is disabled by default.

Usage

N/A

Examples

The following example enables IGP synchronization of BGP static network routes in the router configuration mode:

```
Switch# configure terminal  
Switch(config)# router bgp 11
```

```
Switch(config-router)# network synchronization
```

Related Commands

N/A

6.7.70 Synchronization

Command Purpose

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.

Use the `no` parameter with this command to disable this function.

Command Syntax

synchronization

no synchronization

Command Mode

Router Configuration

Address Family Configuration

Default

IGP synchronization is disabled.

Usage

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems. The `no synchronization` command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

Examples

The following example enables IGP synchronization of BGP static network routes in the IPv4-Unicast address family:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv4 unicast
Switch(config-af)# network synchronization
```

Related Commands

N/A

6.7.71 router bgp

Command Purpose

Use this command to configure a BGP routing process.

Use the no parameter with this command to disable a routing process.

Command Syntax

router bgp *ASN*

no router bgp *ASN*

Parameter	Parameter Description	Parameter Value
ASN	Specifies the Autonomous System (AS) number	1-4294967295

Command Mode

Global Configuration

Default

N/A

Usage

The router bgp command enables a BGP routing process.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)#
```

Related Commands

N/A

6.7.72 show debugging bgp

Command Purpose

Use this command to display the BGP debugging option set.

Command Syntax

```
show debugging bgp
```

Command Mode

Privileged EXEC

Default

N/A

Usage

None

Examples

```
Switch# show debugging bgp
```

Related Commands

N/A

6.7.73 show ip bgp

Command Purpose

Use this command to display BGP network information.

Command Syntax

```
show ip bgp ( IPADDRESS | )
```

```
show ip bgp ipv4 PREFIX ( IPADDRESS | )
```

Parameter	Parameter Description	Parameter Value
IPADDRESS	A.B.C.D A.B.C.D/M Specifies the address and length.	IPv4 Address in A.B.C.D format or IPv4 Address and mask length in A.B.C.D/M format

Parameter	Parameter Description	Parameter Value
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp 10.10.1.34/24
```

Related Commands

N/A

6.7.74 show ip bgp attribute-info

Command Purpose

Use this command to show bgp attribute information.

Command Syntax

```
show ip bgp attribute-info
```

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp attribute-info command displaying internal attribute information:

```
Switch# show ip bgp attribute-info
```

Related Commands

N/A

6.7.75 show ip bgp cidr-only**Command Purpose**

Use this command to display routes with non-natural network masks.

Command Syntax

```
show ip bgp cidr-only
```

```
show ip bgp ipv4 PREFIX cidr-only
```

Parameter	Parameter Description	Parameter Value
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp cidr-only command:

```
Switch# show ip bgp cidr-only
```

Related Commands

N/A

6.7.76 show ip bgp community**Command Purpose**

Use this command to display routes matching the communities.

Command Syntax

```
show ip bgp community TYPE ( exact-match | )
```

```
show ip bgp ipv4 PREFIX community TYPE ( exact-match | )
```

Parameter	Parameter Description	Parameter Value
TYPE	AA:NN local-AS no-advertise no-export	-
AA:NN	Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.	AA is in the range 1-65535 NN is in the range of 1-65535
local-AS	Do not send outside local AS (well-known community).	-
no-advertise	Do not advertise to any peer (well-known community).	-
no-export	Do not export to next AS (well-known community).	-
exact-match	Specifies that display the exact match of the communities.	-
PREFIX	(multicast unicast)	-
multicast	Specifies a IPv4 multicast address family.	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp community 10:23 exact-match
Switch# show ip bgp ipv4 multicast community 10:23 exact-match
```

Related Commands

N/A

6.7.77 show ip bgp community-info**Command Purpose**

Use this command to list all BGP community information.

Command Syntax

```
show ip bgp community-info
```

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp community-info
```

Related Commands

N/A

6.7.78 show ip bgp community-list

Command Purpose

Use this command to display routes that match the community-list.

Command Syntax

```
show ip bgp community-list LISTNAME ( exact-match | )
```

```
show ip bgp ipv4 PREFIX community-list LISTNAME ( exact-match | )
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the community list name.	Up to 20 characters
exact-match	Displays only routes that have exactly the same specified communities.	-
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp community-list mylist exact-match
Switch# show ip bgp ipv4 unicast community-list mylist
```

Related Commands

N/A

6.7.79 show ip bgp dampening

Command Purpose

Use this command to display detailed information about dampening.

Command Syntax

show ip bgp dampening (dampened-paths | flap-statistics | parameters)

show ip bgp ipv4 *PREFIX* dampening (dampened-paths | flap-statistics | parameters)

Parameter	Parameter Description	Parameter Value
dampened-paths	Display paths suppressed due to dampening.	-
flap-statistics	Display flap statistics of routes.	-
parameters	Display details of configured dampening parameters.	-
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Enable bgp dampening to maintain dampened-path information in memory. The following is a sample output displaying all the dampening parameters:

```
Switch# show ip bgp dampening parameters
```

Related Commands

N/A

6.7.80 show ip bgp filter-list

Command Purpose

Use this command to display routes conforming to the filter-list.

Command Syntax

```
show ip bgp filter-list LISTNAME
```

```
show ip bgp ipv4 PREFIX filter-list LISTNAME
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the regular-expression access list name.	Up to 20 characters
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed. Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp filter-list mylist
Switch# show ip bgp ipv4 unicast filter-list Switch
```

Related Commands

N/A

6.7.81 show ip bgp inconsistent-as

Command Purpose

Use this command to display routes with inconsistent AS Paths.

Command Syntax

```
show ip bgp inconsistent-as
```

```
show ip bgp ipv4 PREFIX inconsistent-as
```

Parameter	Parameter Description	Parameter Value
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp inconsistent-as
Switch# show ip bgp ipv4 unicast inconsistent-as
```

Related Commands

N/A

6.7.82 show ip bgp neighbors

Command Purpose

Use this command to display detailed information on TCP and BGP neighbor connections.

Command Syntax

show ip bgp neighbors (*IPADDRESS* (advertised-routes | *RECEIVED* | received-routes | routes) |)

show ip bgp ipv4 *PREFIX* neighbors (*IPADDRESS* (advertised-routes | received | received-routes | routes) |)

Parameter	Parameter Description	Parameter Value
IPADDRESS	Specifies an IPv4 address.	IPv4 Address in A.B.C.D format
advertised-routes	Displays the routes advertised to a BGP neighbor.	-
received	received prefix-filter Displays all received routes, both accepted and rejected.	-
prefix-filter	Displays the prefix-list filter.	-
received-routes	Displays the received routes from neighbor. To display all the received routes from the neighbor, configure the BGP soft reconfigure first. routes Displays all accepted routes learned from neighbors.	-
routes	Display routes learned from neighbor	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp neighbors command displaying information about the specified neighbor:

```
Switch# show ip bgp neighbors
```

Related Commands

N/A

6.7.83 show ip bgp paths

Command Purpose

Use this command to display BGP path information.

Command Syntax

show ip bgp paths

show ip bgp ipv4 *PREFIX* paths

Parameter	Parameter Description	Parameter Value
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp paths
```

Related Commands

N/A

6.7.84 show ip bgp prefix-list

Command Purpose

Use this command to display routes matching the prefix-list.

Command Syntax

```
show ip bgp prefix-list LIST
```

```
show ip bgp ipv4 PREFIX prefix-list LIST
```

Parameter	Parameter Description	Parameter Value
LIST	Specifies the name of the IP prefix list.	Up to 40 characters
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp prefix-list mylist
```

Related Commands

N/A

6.7.85 show ip bgp quote-regexp

Command Purpose

Use this command to display routes matching the AS path regular expression in quotes.

Command Syntax

show ip bgp quote-regexp *LINE*

show ip bgp ipv4 *PREFIX* quote-regexp *LINE*

Parameter	Parameter Description	Parameter Value
LINE	Specifies a regular-expression to match the BGP AS paths	A regular-expression in quote
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp quote-regexp "Switch"
```

Related Commands

N/A

6.7.86 show ip bgp regexp

Command Purpose

Use this command to display routes matching the AS path regular expression.

Command Syntax

show ip bgp regexp *LINE*

show ip bgp ipv4 *PREFIX* regexp *LINE*

Parameter	Parameter Description	Parameter Value
regexp	Displays routes matching the AS path regular expression.	-
LINE	Specifies a regular expression to match the BGP AS paths.	A regular-expression
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp regexp myexpression
```

Related Commands

N/A

6.7.87 show ip bgp scan

Command Purpose

Use this command to display BGP scan status.

Command Syntax

show ip bgp scan

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show ip bgp scan
```

Related Commands

N/A

6.7.88 show ip bgp summary

Command Purpose

Use this command to display a summary of BGP neighbor status.

Command Syntax

show ip bgp summary

show ip bgp ipv4 *PREFIX* summary

Parameter	Parameter Description	Parameter Value
ipv4	Specifies the address family. The type of address family determines the routing table that is displayed.	-
PREFIX	(multicast unicast)	-

Parameter	Parameter Description	Parameter Value
unicast	Specifies a IPv4 unicast address family. This is the default option.	-
multicast	Specifies a IPv4 multicast address family.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp summary command displaying a summary of BGP neighbor status:

```
Switch# show ip bgp summary
```

Related Commands

N/A

6.7.89 show ip bgp vpnv4 all

Command Purpose

Use this command to display VPNv4 NLRI specific information.

Command Syntax

show ip bgp vpnv4 all *TYPE*

Parameter	Parameter Description	Parameter Value
all	Displays information about all VPNv4 NRIs	-
TYPE	(A.B.C.D neighbors summary)	-
neighbors	Displays information about BGP neighbors.	-
summary	Displays summary of the BGP neighbor status.	-

Parameter	Parameter Description	Parameter Value
A.B.C.D	Network for which information will be displayed in the BGP routing table.	IPv4 Address in A.B.C.D format

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp vpnv4 all command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 all
```

Related Commands

N/A

6.7.90 show ip bgp vpnv4 rd

Command Purpose

Use this command to display VPNv4 NLRI specific information.

Command Syntax

show ip bgp vpnv4 rd *WORD TYPE*

Parameter	Parameter Description	Parameter Value
rd	Display information for a route distinguisher	-
WORD	VPN Route Distinguisher	Up to 15 characters
TYPE	(A.B.C.D neighbors summary)	-
neighbors	Displays information about BGP neighbors.	-
summary	Displays summary of the BGP neighbor status.	-

Parameter	Parameter Description	Parameter Value
A.B.C.D	Network for which information will be displayed in the BGP routing table.	IPv4 Address in A.B.C.D format

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp vpnv4 rd command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 rd 123
```

Related Commands

N/A

6.7.91 show ip bgp vpnv4 vrf

Command Purpose

Use this command to display VPNv4 NLRI specific information.

Command Syntax

show ip bgp vpnv4 vrf *WORD TYPE*

Parameter	Parameter Description	Parameter Value
vrf	VPN Routing/Forwarding instance	-
WORD	VPN Routing/Forwarding instance name	Up to 15 characters
TYPE	(A.B.C.D neighbors summary)	-
neighbors	Displays information about BGP neighbors.	-
summary	Displays summary of the BGP neighbor status.	-

Parameter	Parameter Description	Parameter Value
A.B.C.D	Network for which information will be displayed in the BGP routing table.	IPv4 Address in A.B.C.D format

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show ip bgp vpnv4 rd command displaying VPNv4 specific information:

```
Switch# show ip bgp vpnv4 vrf 123
```

Related Commands

N/A

6.7.92 timers

Command Purpose

Use this command sets the BGP keepalive timer and holdtime timer values.

Use the no parameter with this command to reset timers to default value.

Command Syntax

timers bgp *KEEPALIVE HOLDTIME*

no timers bgp

Parameter	Parameter Description	Parameter Value
KEEPALIVE	<0-65535> The frequency with which the keepalive messages are sent to the neighbors. The default value is 60 seconds.	0-65535
HOLDTIME	The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 180 seconds.	3-65535

Command Mode

Router Configuration

Default

N/A

Usage

This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# timers bgp 40 120
```

Related Commands

N/A

6.8 ISIS Commands

6.8.1 accept-lifetime

Command Purpose

Use this command to specify the time period during which the authentication on a key chain is received as valid.

Use the no parameter with this command to negate this command.

Command Syntax

accept-lifetime HH:MM:SS DAY MONTH YEAR HH1:MM1:SS1 DAY1 MONTH1 YEAR1

accept-lifetime HH:MM:SS MONTH DAY YEAR infinite

accept-lifetime HH:MM:SS MONTH DAY YEAR duration <1-2147483646>

no accept-lifetime

Parameter	Parameter Description	Parameter Value
HH:MM:SS	Specify the end time of accept-lifetime in hours, minutes and seconds.	0-23:0-59:0-59
DAY	Specify the day of the month to end.	1-31
MONTH	Specify the month of the year to end as the first three letters of the month, for example, december.	january, february, march, april, may, june, july, august, september, october, november, december

Parameter	Parameter Description	Parameter Value
YEAR	Specify the year to end.	1993-2035
HH1:MM1:SS1		0-23:0-59:0-59
DAY1		1-31
MONTH1		january, february, march, april, may, june, july, august, september, october, november, december
YEAR1		1993-2035
<1-2147483646>	Specify the actual end time duration of a key in seconds.	1-2147483646

Command Mode

Key Chain Configuration

Default

None

Usage

None

Examples

The follow example shows how to specify the time period during which the authentication on a key chain is received as valid.:

```
Switch# configure terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

Related Commands

None

6.8.2 address-family ipv6

Command Purpose

Use this command to enter ‘address-family ipv6’ mode, where users can configure IPv6 routing specific configuration.

Use the no parameter with this command to remove all configuration under ‘address-family ipv6’.

Command Syntax

address-family ipv6 (unicast |)

no address-family ipv6 (unicast |)

Parameter	Parameter Description	Parameter Value
unicast	Specify unicast routing for IPv6.	-

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to enter 'address-family ipv6' mode:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# address-family ipv6 unicast
Switch(config-router-af)#
```

Related Commands

None

6.8.3 adjacency-check

Command Purpose

Use this command to configure the policy of adjacency based on the protocol related TLVs in the Hello packet. Check adjacency with protocol related TLVs including Protocols Supported TLV or IP Interface Address TLV by default. The command with no parameter disables this check.

Use the no parameter with this command to disable the adjacency check.

Command Syntax

adjacency-check
no adjacency-check

Command Mode

Router Configuration

Address Family Configuration

Default

Enabled

Usage

None

Examples

The following example shows how to enable adjacency check:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router-af)# adjacency-check
```

Related Commands

None

6.8.4 area-password

Command Purpose

Use this command to set the authentication password for the Level-1 area and to set authentication on Level-1 SNP PDUs. This command enables authentication when receiving and sending LSP and SNP PDU in Level-1 areas. Area password must be the same for all the routers in the same area.

Use the no parameter with this command to clear the area password.

Command Syntax

area-password *PASSWORD*

area-password *WORD* authenticate snp (send-only | validate)

no area-password

Parameter	Parameter Description	Parameter Value
PASSWORD	Specify the password string.	Up to 254 characters
authenticate	Specify to insert the password into Level-1 SNP PDUs.	-
snp	Specify the sequence number PDU (SNP).	-
send-only	Specify to only insert the password into the Level-1 SNP PDUs, but not check the password in SNP PDUs that it receives. Use this keyword during a software upgrade to ease the transition.	-

Parameter	Parameter Description	Parameter Value
validate	Specify to insert the password into the Level-1 SNP PDUs and check the password in SNPs that it receives.	-

Command Mode

Router Configuration

Default

Not configured

Usage

None

Examples

The following example shows how to set the authentication password for the Level-1 area:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# area-password code1234

Switch(config-router)# no area-password
```

Related Commands

None

6.8.5 authentication key-chain

Command Purpose

Use this command to set the key chain to be used for authentication at the instance level. Authentication mode must be set to md5 to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed.

Only one authentication key-chain is applied to an interface at a time. That is, issuing a second isis authentication key-chain command overrides the first isis authentication key-chain command. Authentication can be specified for an individual interface using the isis authentication key-chain command.

Use the no parameter with this command to unset the key chain used for authentication.

Command Syntax

authentication key-chain *WORD* (level-1 | level-2 |)

no authentication key-chain *PASSWORD* (level-1 | level-2 |)

no authentication key-chain (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
WORD	Specify the chain name (valid authentication keys).	A String of key chain name
level-1	Specify an authentication key-chain for level-1 PDUs.	-
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Router Configuration

Default

Disabled

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the key chain to be used for authentication at the level-1:

```
Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication key-chain code1234 level-1
```

Related Commands

None

6.8.6 authentication mode md5

Command Purpose

Use this command to set the MD5 authentication mode at the instance level.

If clear-text authentication was configured using the area-password or domain-password commands, the authentication mode command overrides both of those commands (based on the level at which MD5 is configured). If the authentication mode command was used first, and subsequently an attempt is made to use the area-password or domain-password commands, the attempt fails. To configure clear-text authentication using the area-password or domain-password commands, first use the no authentication mode command.

The type of authentication and the level to which it applies can be specified for a single interface, rather than per instance, using the isis authentication mode command.

Use the no parameter with this command to unset the MD5 authentication mode.

Command Syntax

authentication mode (md5 | text) (level-1 | level-2 |)

no authentication mode (md5 | text) (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
md5	Keyed message digest	-
text	Text mode	-
level-1	Specify an authentication key-chain for level-1 PDUs.	-
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Router Configuration

Default

Disabled

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the MD5 authentication mode at the level-1:

```
Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication mode md5 level-1
Switch(config-router)# no authentication mode md5 level-1
```

Related Commands

None

6.8.7 authentication send-only

Command Purpose

Use this command to set the send-only option at the instance level.

Use this command before configuring the authentication mode and authentication key-chain, so that the implementation of authentication goes smoothly.

After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then, specify the no authentication send-only command to disable the send-only feature.

If neither the level-1 nor level-2 keyword is configured, the send-only feature applies to both levels. The send-only option applies to both levels if no level is specified.

Use the no parameter with this command to unset the send-only option.

Command Syntax

authentication send-only (level-1 | level-2 |)

no authentication send-only (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
level-1	Specify an authentication key-chain for level-1 PDUs.	-
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Router Configuration

Default

Disabled

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the send-only option at the level-1.:

```
Switch# configure terminal
Switch(config)# router isis 1
Switch(config-router)# authentication send-only level-1
Switch(config-router)# no authentication send-only level-1
```

Related Commands

None

6.8.8 bfd all-interfaces

Command Purpose

Use this command to enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.

This command sets BFD fall-over check for all the neighbors under specified process. To disable BFD checking on particular interface use `isis bfd disable` command at interface mode.

Use the `no` parameter with this command to disable BFD functionality for an instance.

Command Syntax

```
bfd all-interfaces  
no bfd all-interfaces
```

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to enable the BFD feature on the interfaces enabled with this ISIS instance.:

```
Switch# configure terminal  
Switch(config)# router isis  
Switch(config-router)# bfd all-interfaces
```

Related Commands

None

6.8.9 clear clns neighbors

Command Purpose

Use this command to clear CLNS neighbor adjacencies.

Command Syntax

```
clear clns neighbors
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The example shows how to clear CLNS neighbor adjacencies.:

```
Switch# clear clns neighbors
```

Related Commands

None

6.8.10 clear clns is-neighbors

Command Purpose

Use this command to clear IS neighbor adjacencies.

Command Syntax

clear clns is-neighbors *System-ID*

Parameter	Parameter Description	Parameter Value
System-ID	Neighbor system ID in XXXX.XXXX.XXXX format.	hexadecimal

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The example shows how to clear IS neighbor adjacencies.:

```
Switch# clear clns is-neighbors 1234.789A.BCDF
```

Related Commands

None

6.8.11 clear ip isis route

Command Purpose

Use this command to clear IPv4 routes.

Command Syntax

clear ip isis (*INSTANCE* |) route (redistribution | all)

Parameter	Parameter Description	Parameter Value
INSTANCE	Routing area tag.	Up to 20 characters
redistribution	Clear ISIS local redistribution routes.	-
all	Clear all of the ISIS routing tables.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The example shows how to clear ISIS IPv4 routes.:

```
Switch# clear ip isis route all
```

Related Commands

None

6.8.12 clear isis counter

Command Purpose

Use this command to clear system-wide IS-IS counters

Command Syntax

```
clear isis counter
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The example shows how to clear system-wide IS-IS counters.:

```
Switch# clear isis counter
```

Related Commands

None

6.8.13 clear isis interface counter

Command Purpose

Use this command to clear interface counters.

Command Syntax

```
clear isis interface counter ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
<i>IFNAME</i>	Interface name.	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

If you do not specify a parameter, then counters for all interfaces are cleared.

Examples

The example shows how to clear clear interface counters.:

```
Switch# clear isis interface counter
```

Related Commands

None

6.8.14 clear isis process**Command Purpose**

Use this command to restart ISIS processes.

Command Syntax

clear isis (*INSTANCE* |) process

Parameter	Parameter Description	Parameter Value
INSTANCE	Routing area tag.	Up to 20 characters

Command Mode

Privileged EXEC

Default

None

Usage

If you do not specify a parameter, then all ISIS processes are restarted.

Examples

The example shows how to restart ISIS processes.:

```
Switch# clear isis process
```

Related Commands

None

6.8.15 debug isis

Command Purpose

Use this command to turn on debugging for specified criteria. Debug commands enable to show some debugging information about specified criteria into file or terminal.

Use the no parameter to turn off debugging for specified criteria.

Command Syntax

```
debug isis ( all | )
```

```
debug isis ( authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
```

```
no debug isis ( all | )
```

```
no debug all
```

```
no debug all isis
```

```
undebug all
```

```
undebug isis ( all | )
```

```
undebug all isis
```

```
no debug isis ( authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
```

```
undebug isis ( authentication | bfd | checksum | events | hello ( interface IFNAME | System-ID | ) | ifsm | local-updates | lsp | nfsm | nsm | pdu | protocol-errors | spf )
```

Parameter	Parameter Description	Parameter Value
all	Enables all debugging.	-
authentication	Debugging for authentication.	-
checksum	Debugging for checksums.	-
bfd	Debugging for bidirectional forwarding detection.	-
events	Debugging for internal events.	-
hello	Debugging for hello processing.	-
interface	Interface.	-

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name.	Support physical/aggregation/loopback/vlan/tunnel ports
System-ID	System identifier.	-
ifsm	Debugging for interface finite state machine.	-
local-updates	Debugging for local updates.	-
lsp	Debugging for label switched path.	-
nfsm	Debugging for neighbor finite state machine.	-
nsm	Debugging for NSM messages.	-
pdu	Debugging for protocol data unit.	-
protocol-errors	Debugging for protocol errors.	-
spf	Debugging for shortest path first route calculation.	-

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

The example shows how to enable all isis debugging.:

```
Switch# debug isis all
```

Related Commands

None

6.8.16 default-information originate

Command Purpose

Use this command to originate reachability information to Default destination into LSP. There is no default information in Level-2 domain by default, while Level-1 router calculates default to L1L2 route SPF calculation. This command enables to originate default route into Level-2 domain.

Use the no parameter with this command to withdraw reachability information to default destination from LSP.

Command Syntax

default-information originate

no default-information originate

Parameter	Parameter Description	Parameter Value
originate	Specify to distribute a default route	-

Command Mode

Router Configuration

Address Family Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to originate reachability information to Default destination into LSP both ipv4 and ipv6:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# default-information originate
Switch(config-router)# address-family ipv6
Switch(config-router-af)# default-information originate
```

Related Commands

None

6.8.17 distance

Command Purpose

Use this command in router mode to set the administrative distance for all IPv4 routes.

Use the no parameter with this command to remove an administrative distance.

Command Syntax

distance *DISTANCE* (*System-ID* (*ACL* |) |)

no distance ((*System-ID* | *System-ID* *ACL*) |)

Parameter	Parameter Description	Parameter Value
DISTANCE	Distance range.	1-255
System-ID	Source ID in XXXX.XXXX.XXXX format.	hexadecimal
ACL	Access-list name.	Up to 40 characters

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to set the administrative distance for all ISIS IPv4 routes:

```
Switch# configure terminal
Switch(config)# router isis
Switch(config-router)# distance 40
```

Related Commands

None

6.8.18 domain-password

Command Purpose

Use this command to set the authentication password for the Level-2 domain, and optionally, the authentication password on Level-2 SNP PDUs. Configuring this command to enable authentication when receiving and sending LSP and SNP PDU in Level-2 domain. Domain password must be the same in Level-2 domain.

Use the no parameter with this command to clear the domain password.

Command Syntax

domain-password *PASSWORD*

domain-password *PASSWORD* authenticate snp (send-only | validate)

no domain-password

Parameter	Parameter Description	Parameter Value
PASSWORD	The password string.	Up to 254 characters
authenticate	Inserts the password into Level-2 SNP PDUs.	-
snp	SNP PDUs.	-
send-only	Only inserts the password into the Level-2 SNP PDUs, but does not check the password in SNP PDUs that it receives. Use this keyword during a software upgrade to ease the transition.	-
validate	Inserts the password into the Level-2 SNP PDUs, and checks the password in SNP PDUs that it receives.	-

Command Mode

Router Configuration

Default

By default, there is no domain password.

Usage

None

Examples

The following example shows how to set the authentication password for the Level-2 domain:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# domain-password mypasswd

Switch(config-router)# no domain-password
```

Related Commands

None

6.8.19 ignore-lsp-errors

Command Purpose

Use this command to ignore LSPs with checksum errors. By default, validates checksum for LSP whenever it receives LSPs and if the checksum has an error, the LSP will be dropped. Configuring this command to ignore the LSP checksum error and treat it as if checksum is passed.

Use the no parameter to turn off this function.

Command Syntax

```
ignore-lsp-errors  
no ignore-lsp-errors
```

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to ignore LSPs with checksum errors:

```
Switch# configure terminal  
Switch(config)# router isis bb  
Switch(config-router)# ignore-lsp-errors
```

Related Commands

None

6.8.20 ip route high-priority tag

Command Purpose

Use this command to set a high priority tag value.

Use the no parameter to turn off this function.

Command Syntax

```
ip route high-priority tag TAG  
no ip route high-priority tag
```

Parameter	Parameter Description	Parameter Value
TAG	Tag value	1-4294967295

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to set a high priority tag value.:

```
Switch# configure terminal
Switch(config)# router isis A
Switch(config-router)# ip route high-priority tag 500
```

Related Commands

None

6.8.21 ip router isis

Command Purpose

Use this command to enable IPv4 routing on the interface. This command is mandatory to configuration. Match the instance tag to one of existing instance' s tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface.

Configuring this command, the router sends Hello with IP address TLV on this interface, and IP reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable IPv4 routing on the interface. This action does not clear the database. To clear the database, unconfigure the routing instance.

Command Syntax

ip router isis (*INSTANCE* |)

no ip router isis (*INSTANCE* |)

Parameter	Parameter Description	Parameter Value
INSTANCE	instance name.	Up to 20 characters

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to enable ISIS IPv4 routing on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip router isis bb
```

Related Commands

None

6.8.22 ipv6 router isis

Command Purpose

Use this command to enable IPv6 routing on the interface. This command is mandatory to IPv6 configuration. Match the instance tag to one of existing instance's tags, or a new instance with the tag name should be initiated, otherwise routing will not run on this interface. Configuring this command, the router sends Hello with IPv6 address TLV on this interface, and IPv6 reachability information TLV in the LSP will be updated.

Use the no parameter with this command to disable IPv6 routing on the interface.

Command Syntax

```
ipv6 router isis ( INSTANCE | )
no ipv6 router isis ( INSTANCE | )
```

Parameter	Parameter Description	Parameter Value
INSTANCE	instance name.	Up to 20 characters

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to enable ISIS IPv6 routing on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 router isis bb
```

Related Commands

None

6.8.23 isis authentication key-chain

Command Purpose

Use this command to set the key chain to be used for authentication on the interface-related packets.

Authentication mode must be set to md5 or text to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed. Only one authentication key-chain is applied to an interface at a time. That is, issuing a second isis authentication key-chain command overrides the first isis authentication key-chain command.

If neither the level-1 nor level-2 keyword is configured, the key chain applies to the level(s) on which the authentication mode is configured as md5. Authentication can be specified for an entire, instead of at the interface level, by using the authentication key-chain command.

Use the no parameter with this command to unset the key chain used for authentication on the interface-related packets.

Command Syntax

isis authentication key-chain *KEY_NAME* (level-1 | level-2 |)

no isis authentication key-chain (level-1 | level-2 |)

no isis authentication key-chain *KEY_NAME* (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
KEY_NAME	Chain name - valid authentication keys.	A String of key chain name
level-1	Specify an authentication key-chain for level-1 PDUs.	-
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Interface Configuration

Default

Disabled

Usage

The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Examples

The following example shows how to set the key chain to be used for authentication on the interface-related packets:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis authentication key-chain code1234 level-1
```

Related Commands

None

6.8.24 isis authentication mode md5

Command Purpose

Use this command to set the MD5 authentication mode. If clear text authentication was configured using the isis password command, the isis authentication mode command overrides the isis password command. If the isis authentication mode command was used, then subsequently an attempt is made to use the isis password command, the attempt fails.

To configure clear text authentication using the isis password command, first use the no isis authentication mode command. The type of authentication and the level to which it applies can be specified for the entire instance, rather than per interface, using the authentication mode command.

Use the no parameter with this command to unset the MD5 authentication mode.

Command Syntax

isis authentication mode (md5 | text) (level-1 | level-2 |)

no isis authentication mode (md5 | text) (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
md5	Keyed message digest	-
text	Text mode	-
level-1	Specify an authentication key-chain for level-1 PDUs.	-

Parameter	Parameter Description	Parameter Value
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Interface Configuration

Default

Disabled

Usage

The send-only option applies to both levels if no level is specified.

Examples

The following example shows how to set the MD5 authentication mode.:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis authentication mode md5
```

Related Commands

None

6.8.25 isis authentication send-only

Command Purpose

Use this command to set the send-only option to the interface-related packets.

Use this command before configuring the ISIS authentication mode and ISIS authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received.

After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.

Use the no parameter with this command to unset the send-only option to the interface-related packets.

Command Syntax

isis authentication send-only (level-1 | level-2 |)

no isis authentication send-only (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
level-1	Specify an authentication key-chain for level-1 PDUs.	-
level-2	Specify an authentication key-chain for level-2 PDUs.	-

Command Mode

Interface Configuration

Default

Disabled

Usage

The send-only option applies to both levels if no level is specified.

Examples

The following example shows how to set the send-only option to the interface-related packets.:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis authentication send-only
```

Related Commands

None

6.8.26 isis bfd

Command Purpose

Use this command to enable/disable the BFD check on interface.

The isis bfd command allows a user to enable BFD on an interface. The isis bfd disable command disables BFD checking on an interface. However, the no isis bfd and no isis bfd disable commands both remove the enable/disable configuration, but do not disable/enable BFD. The bfd all-interfaces command enables BFD on all interfaces attached to an instance then configuring. This command disables BFD configuration on a particular interface.

Command Syntax

```
isis bfd ( disable | )
no isis bfd ( disable | )
```

Parameter	Parameter Description	Parameter Value
disable	Specify to disable BFD.	-

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

The following example shows how to disable bfd on ISIS interface.:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis bfd disable
```

Related Commands

None

6.8.27 isis circuit-type**Command Purpose**

Use this command to set the circuit type for the interface.

If level-1 or level-2-only is specified in this command, sends only the specified level of PDUs.

Use the no parameter to reset circuit type to the default.

Command Syntax

isis circuit-type (level-1 | level-1-2 | level-2-only)

no isis circuit-type

Parameter	Parameter Description	Parameter Value
level-1	Specify that only Level-1 adjacencies are formed.	-
level-1-2	Specify that Level-1-2 adjacencies are formed.	-

Parameter	Parameter Description	Parameter Value
level-2-only	Specify that only Level-2 adjacencies are formed.	-

Command Mode

Interface Configuration

Default

Enabled level-1 and level-2.

Usage

None

Examples

The following example shows how to set the circuit type for the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis circuit-type level-2-only
```

Related Commands

None

6.8.28 isis csnp-interval

Command Purpose

Use this command to set CSNP (Complete sequence number PDU) interval in seconds.

Configuring this command changes the interval between two consecutive CSNP transmission. By default, CSNP is sent every 10 seconds only by LAN DIS. This parameter is only valid on broadcast interface, since periodic CSNP is only sent on broadcast interface, while CSNP on Point-to-Point interface is sent only when adjacency is initiated.

Use the no parameter with this command to reset CSNP interval to the default value.

Command Syntax

isis csnp-interval *INTERVAL* (level-1 | level-2 |)

no isis csnp-interval (level-1 | level-2 |)

no isis csnp-interval <1-65535> (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify the CSNP interval in seconds.	1-65535

Parameter	Parameter Description	Parameter Value
level-1	Specify Level-1 CSNP.	-
level-2	Specify Level-2 CSNP.	-

Command Mode

Interface Configuration

Default

10 seconds level-1 and level-2.

Usage

None

Examples

The following example shows how to set CSNP (Complete sequence number PDU) interval.:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis csnp-interval 20
```

Related Commands

None

6.8.29 isis hello

Command Purpose

Use this command to configure the padding of the Hello packet. pads the Hello packet by default to notify neighbors of the supported MTU size.

Use the no parameter with this command to disable the padding.

Command Syntax

isis hello padding
no isis hello padding

Parameter	Parameter Description	Parameter Value
padding	Specify pad hello packets	-

Command Mode

Interface Configuration

Default

By default, pads the Hello packet.

Usage

None

Examples

The following example shows how to configure the padding of the Hello packet.:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis hello padding
```

Related Commands

None

6.8.30 isis hello-interval

Command Purpose

Use this command to set the Hello interval in seconds. The Hello-interval is set with the hello-multiplier (see isis hello-multiplier command).

Configuring this command changes the time interval between two consecutive Hello transmissions. If a device receives its own LSP with a maximum sequence number, then it suspends for the hold interval. DIS sends Hello transmissions at three times the rate than non-DIS. If is elected as DIS on this interface, sends Hello every 3.3 seconds.

If minimal keyword is specified, Holding timer in Hello PDU is set to 1 second and Hello interval is calculated by dividing by the hello-multiplier. For example, if the hello-multiplier is configured as 4 and hello-interval minimal is the command used, an Hello PDU is sent every 250 milliseconds.

Use the no parameter to set the Hello interval to the default.

Command Syntax

isis hello-interval *INTERVAL* (level-1 | level-2 |)

isis hello-interval minimal (level-1 | level-2 |)

no isis hello-interval (level-1 | level-2 |)

no isis hello-interval <1-65535> (level-1 | level-2 |)

no isis hello-interval minimal (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify the hello interval in seconds.	1-65535

Parameter	Parameter Description	Parameter Value
minimal	Specify the holding-time as 1 second.	-
level-1	Specify Level-1 CSNP.	-
level-2	Specify Level-2 CSNP.	-

Command Mode

Interface Configuration

Default

By default, uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the Hello interval.:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis hello-interval 5 level-1
```

Related Commands

isis hello-multiplier

6.8.31 isis hello-multiplier

Command Purpose

Use this command to set multiplier for Hello holding time.

Changes Holding Timer in Hello PDU. Holding timer is calculated by "Hello-Interval" multiplied by this value. If minimal keyword is specified with the Hello-Interval, the holding timer is set to 1 second and the hello-interval is calculated by dividing 1 by this value.

Use the no parameter with this command to set multiplier to the default.

Command Syntax

```
isis hello-MULTIPLIER <2-100> ( level-1 | level-2 | )
no isis hello-multiplier ( level-1 | level-2 | )
no isis hello-multiplier <2-100> ( level-1 | level-2 | )
```

Parameter	Parameter Description	Parameter Value
MULTIPLIER	Specify a hello multiplier value.	2-100
level-1	Specify Level-1 hello.	-
level-2	Specify Level-2 hello.	-

Command Mode

Interface Configuration

Default

By default, uses 3 seconds for the multiplier value and the multiplier is applied to both level-1 and level-2.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set multiplier for Hello holding time:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis hello-multiplier 4
```

Related Commands

None

6.8.32 isis lsp-interval

Command Purpose

Use this command to set the Link State Packet (LSP) transmission interval.

Configuring this command changes the minimum interval between two consecutive LSP transmission. When flooding or some other event triggers LSP to transmit, the LSP is put on the interface queue and scheduled to transmit according to this interval. Two consecutive LSP transmissions are scheduled to have at least this interval.

Use the no parameter with this command to set LSP transmission interval to the default.

Command Syntax

isis lsp-interval *INTERVAL*

no isis lsp-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify an LSP transmission interval in milliseconds.	1-4294967295

Command Mode

Interface Configuration

Default

By default, 33 milliseconds for the interval.

Usage

None

Examples

The following example shows how to set the Link State Packet (LSP) transmission interval:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis lsp-interval 100
```

Related Commands

None

6.8.33 isis mesh-group

Command Purpose

Use this command to set Mesh Group ID on the current interface.

Use the no parameter to unset mesh group on the current interface.

Command Syntax

isis mesh-group *MESH_GROUP*

isis mesh-group blocked

no isis mesh-group

Parameter	Parameter Description	Parameter Value
MESH_GROUP	Specify a mesh group number	1-4294967295

Parameter	Parameter Description	Parameter Value
blocked	Specify to block LSPs on the current interface. If an interface is configured as "mesh group blocked," the standard LSP database synchronization process is applied if the interface receives CSNP or PSNP.	-

Command Mode

Interface Configuration

Default

By default, mesh groups are not enabled on this interface.

Usage

None

Examples

The following example shows how to set Mesh Group ID on the current interface :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis mesh-group 20
```

Related Commands

None

6.8.34 isis metric

Command Purpose

Use this command to set default metric for the interface. The interface default metric is put into IP reachability information TLVs, IS reachability information TLVs and IPv6 reachability TLVs in LSPs. The value is used for SPF calculation.

Use the no parameter with this command to set default metric to the default.

Command Syntax

isis metric *METRIC* (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
METRIC	Specify a default metric.	1-16777214
level-1	Specify default metric for level-1 circuit.	-

Parameter	Parameter Description	Parameter Value
level-2	Specify default metric for level-2 circuit.	-

Command Mode

Interface Configuration

Default

By default, uses 10 for the metric value and the value is applied to both level-1 and level-2.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set default metric for the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis metric 20
```

Related Commands

None

6.8.35 isis network

Command Purpose

Use this command to change a broadcast interface network type to a point-to-point network type.

Use the no parameter with this command to revert to the default setting of a broadcast interface network type.

Command Syntax

isis network point-to-point

no isis network (point-to-point |)

Parameter	Parameter Description	Parameter Value
point-to-point	Specify a point-to-point network.	-

Command Mode

Interface Configuration

Default

This option is disabled by default.

Usage

None

Examples

The following example shows how to change a broadcast interface network type to a point-to-point network type:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis network point-to-point
```

Related Commands

None

6.8.36 isis password

Command Purpose

Use this command to set the authentication password of Hello PDU on the interface.

Use the no parameter to clear the password.

Command Syntax

isis password *PASSWORD* (level-1 | level-2 |)

no isis password (level-1 | level-2 |)

no isis password *PASSWORD* (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
PASSWORD	Specify a password string.	Up to 254 characters
level-1	Specify a password for Level-1 hello PDUs.	-
level-2	Specify a password for Level-2 hello PDUs.	-

Command Mode

Interface Configuration

Default

By default, no password is configured; this applies to both level-1 and level-2.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the authentication password of Hello PDU on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis password mypassWORD level-1
```

Related Commands

None

6.8.37 isis priority

Command Purpose

Use this command to set the priority for LAN DIS election. This command changes the priority value in LAN Hello PDUs. A lower priority value is less preferred in DIS election, and a higher priority value is more preferred.

Command Syntax

isis priority *PRIORITY* (level-1 | level-2 |)

no isis priority (level-1 | level-2 |)

no isis priority <0-127> (level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
PRIORITY	Priority value	0-127
level-1	Specify a priority for Level-1 hello PDUs.	-
level-2	Specify a priority for Level-2 hello PDUs.	-

Command Mode

Interface Configuration

Default

By default, uses 64 for the priority value, and the priority is applied to both level-1 and level-2.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set the priority for LAN DIS election:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# isis priority 127
```

Related Commands

None

6.8.38 isis retransmit-interval

Command Purpose

Use this command to set LSP retransmission interval.
Use the no parameter to set the interval to the default.

Command Syntax

isis retransmit-interval *INTERVAL*

no isis retransmit-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify an interval for retransmission of the same LSP in seconds.	0-65535

Command Mode

Interface Configuration

Default

5 seconds.

Usage

None

Examples

The following example shows how to set LSP retransmission interval:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# isis retransmit-interval 10
Switch(config-if)# no isis retransmit-interval
```

Related Commands

None

6.8.39 isis tag

Command Purpose

Use this command to set the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface. If you do not specify a parameter, then the tag value is set for level-1-2 boundary. Use the no parameter to unset the tag.

Command Syntax

isis tag *TAG* (level-1 | level-2 |)

no isis tag

Parameter	Parameter Description	Parameter Value
TAG	Tag value.	1-4294967295
level-1	Specify the tag value for the level-1 boundary.	-
level-2	Specify the tag value for the level-2 boundary.	-

Command Mode

Interface Configuration

Default

This option is disabled by default.

Usage

None

Examples

The following example shows how to the tag for link-state packets (LSPs) sent out advertising routes for networks directly connected to an interface.:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
Switch(config-if)# isis tag 500 level-1
```

Related Commands

None

6.8.40 ispf

Command Purpose

Use this command to enable incremental SPF for a routing process.
Use the no parameter to disable incremental SPF from a routing process.

Command Syntax

```
ispf
ispf ( level-1 | level-1-2 | level-2-only )
no ispf
```

Parameter	Parameter Description	Parameter Value
level-1	Act as level-1 only IS.	-
level-1-2	Act as level-1-2 IS.	-
level-2-only	Act as level-2 only IS.	-

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to enable incremental SPF for a routing process:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# ispf level-1
```


Related Commands

None

6.8.41 is-type

Command Purpose

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the `is-type` command in router configuration mode.

Use the `no` parameter to set the IS to the default.

Command Syntax

`is-type ( level-1 | level-1-2 | level-2-only )`

`no is-type`

Parameter	Parameter Description	Parameter Value
level-1	Act as level-1 only IS.	-
level-1-2	Act as level-1-2 IS.	-
level-2-only	Act as level-2 only IS.	-

Command Mode

Router Configuration

Default

By default, uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Usage

None

Examples

The following example shows how to configure the routing level for an ISIS instance:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# is-type level-1
```

Related Commands

None

6.8.42 lsp-gen-interval

Command Purpose

Use this command to set minimum interval before regenerating the same LSP. The smaller the interval, the faster the convergence. However, this setting might cause more frequent flooding.

Use the no parameter with this command to set the interval to the default.

Command Syntax

`lsp-gen-interval INTERVAL`

`lsp-gen-interval ( level-1 | level-2 ) <1-120>`

`no lsp-gen-interval`

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify a minimum interval in seconds.	1-120
level-1	Specify an interval for Level-1 IS.	-
level-2	Specify an interval for Level-2 IS.	-

Command Mode

Router Configuration

Default

30 seconds for the interval and the interval is applied to both level-1 and level-2.

Usage

None

Examples

The following example shows how to set minimum interval before regenerating the same LSP:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# lsp-gen-interval 5
```

Related Commands

None

6.8.43 lsp-mtu

Command Purpose

Use this command to set LSP MTU in bytes.

Use the no parameter with this command to set the MTU to the default.

Command Syntax

`lsp-mtu ( level-1 | level-2 | ) MTU`

`no lsp-mtu ( level-1 | level-2 | )`

Parameter	Parameter Description	Parameter Value
MTU	Specify an MTU size	512-1492
level-1	Specify an interval for Level-1 IS.	-
level-2	Specify an interval for Level-2 IS.	-

Command Mode

Router Configuration

Default

None

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to both levels.

Examples

The following example shows how to set LSP MTU in bytes:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# lsp-mtu 555
```

Related Commands

None

6.8.44 lsp-refresh-interval

Command Purpose

Use this command to set the LSP refresh interval.

IP Infusion recommends making the lsp-refresh-interval smaller than max-lsp-lifetime value.

Use the no parameter to set the interval to the default value.

Command Syntax

lsp-refresh-interval *INTERVAL*

no lsp-refresh-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	Specify an LSP refresh interval in seconds.	1-65535

Command Mode

Router Configuration

Default

900 seconds.

Usage

None

Examples

The following example shows how to set the LSP refresh interval:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# lsp-refresh-interval 600

Switch(config-router)# no lsp-refresh-interval
```

Related Commands

None

6.8.45 max-area-addresses

Command Purpose

Use this command to configure additional manual addresses for an IS-IS area.

Use the no parameter to disable the manual addresses.

Command Syntax

max-area-addresses *NUMBER*

no max-area-addresses

Parameter	Parameter Description	Parameter Value
NUMBER	Specify the maximum area address that can be supported	3-127

Command Mode

Router Configuration

Default

3

Usage

None

Examples

The following example shows how to configure additional manual addresses for an IS-IS area:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# max-area-address 4
```

Related Commands

None

6.8.46 max-lsp-lifetime

Command Purpose

Use this command to set the maximum LSP lifetime. You must set max-lsp-lifetime greater than lsp-refreshinterval.

Use the no parameter to set the lifetime to the default.

Command Syntax

max-lsp-lifetime *LIFETIME*

no max-lsp-lifetime

Parameter	Parameter Description	Parameter Value
LIFETIME	Specify an maximum LSP lifetime in seconds.	350-65535

Command Mode

Router Configuration

Default

1200 seconds.

Usage

None

Examples

The following example shows how to set the maximum LSP lifetime:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# max-lsp-lifetime 1500
```

Related Commands

None

6.8.47 metric-style

Command Purpose

Use this command to configure the metric style.

Use the no parameter to set the style to the default style, narrow.

Command Syntax

metric-style (narrow | wide | transition) (level-1 | level-1-2 | level-2 |)

metric-style (narrow | wide) transition (level-1 | level-1-2 | level-2 |)

no metric-style (narrow | wide | transition) (level-1 | level-1-2 | level-2 |)

Parameter	Parameter Description	Parameter Value
narrow	Specify the old style of TLVs with narrow metric.	-
wide	Specify the new style of TLVs to carry wider metric.	-
transition	Accept both styles of TLVs during transition	-
level-1	Specify the level-1 metric style.	-
level-2	Specify the level-2 metric style.	-
level-1-2	Specify the level-1-2 metric style.	-

Command Mode

Router Configuration

Default

By default, uses narrow metric style for level 1 and 2.

Usage

None

Examples

The following example shows how to configure the metric style:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# metric-style wide
```

Related Commands

None

6.8.48 net

Command Purpose

Use this command to configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process, use the net command in router configuration mode. To remove a NET, use the no form of this command.

Use the no parameter to remove the NET.

Command Syntax

net *NET*

no net *NET*

Parameter	Parameter Description	Parameter Value
NET	Specify a network entity title (NET) in 1 to 13 octets	In XX.XXXX. XXXX.XX format

Command Mode

Router Configuration

Default

By default, does not configure a NET and routing is not enabled for the interface.

Usage

None

Examples

The following example shows how to configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for the routing process:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# net 49.0000.0001.0002.0003.00
```

Related Commands

None

6.8.49 passive-interface

Command Purpose

Use this command to suppress routing updates on all interfaces or on a specified interface, which puts the interfaces into passive mode. To advertise passive prefixes in LSP, there is no need to have at an interface configured with ip router isis. Enabling passive interface on an ISIS enabled interface disables ISIS on the interface and makes the interface passive. Use the no parameter with this command to remove interfaces from passive mode

Command Syntax

```
passive-interface ( IFNAME | )
no passive-interface ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Indicates an interface name.	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to suppress routing updates on a specified interface:

```
Switch# configure terminal
Switch(config)# router isis 100
Switch(config-router)# passive-interface eth-0/1
```

Related Commands

None

6.8.50 prc-interval-exp

Command Purpose

Use this command to configure exponential back-off delay between PRC calculations.
Use the no parameter to disable any set exponential back-off delay between PRC calculations.

Command Syntax

```
prc-interval-exp
prc-interval-exp EXP_MIN EXP_MAX
no prc-interval-exp
```

Parameter	Parameter Description	Parameter Value
EXP_MIN	Set the minimum delay between receiving a change to PRC calculation in milliseconds.	0-2147483647
EXP_MAX	Set the maximum delay between receiving a change to PRC calculation in milliseconds.	0-2147483647

Command Mode

Router Configuration

Default

Minimum Delay 500ms, Maximum Delay 50000ms

Usage

None

Examples

The following example shows how to configure exponential back-off delay between PRC calculations:

```
Switch# configure terminal
Switch(config)# router isis
Switch(config-router)# prc-interval-exp 100 10000
```

Related Commands

None

6.8.51 redistribute

Command Purpose

Use this command to redistribute routes from another protocol into the ISIS routing table.

Use the no parameter to disable this function.

Command Syntax

redistribute (connected | static | rip | ospf | bgp) { metric *METRIC* | metrictype (internal | external) | level-1 | level-2 | level-1-2 | route-map *ROUTE_MAP* }

no redistribute (connected | static | rip | ospf | bgp)

Parameter	Parameter Description	Parameter Value
connected	Redistribute connected routes.	-
static	Redistribute static routes.	-
rip	Redistribute RIP routes.	-
ospf	Redistribute OSPF routes.	-
bgp	Redistribute BGP routes.	-
metric	Specify the metric for redistributed routes.	-
METRIC	Specify the IS-IS default metric.	0-4261412864
metric-type	Specify the IS-IS exterior metric type for redistributed routes:	-
internal	Set IS-IS internal metric type.	-
external	Set IS-IS external metric type.	-
level-1	IS-IS Level-1 routes.	-
level-2	IS-IS Level-2 routes.	-
level-1-2	IS-IS Level-1 and Level-2 routes.	-

Parameter	Parameter Description	Parameter Value
route-map	Specify a Route map reference.	-
ROUTE_MAP	Specify name of the route-map.	Up to 20 characters

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to redistribute routes from another protocol into the ISIS routing table:

```
Switch# configure terminal
Switch(config)# router isis A
Switch(config-router)# redistribute bgp metric 12
```

Related Commands

None

6.8.52 redistribute isis

Command Purpose

Use this command to redistribute reachability information from one level to the other level. If an distribute-list name is given with this command for an access list that does not exist, the routes are still redistributed.

Use the no parameter with this command to stop redistribution.

Command Syntax

```
redistribute isis level-1 into level-2
redistribute isis level-2 into level-1
redistribute isis level-1 into level-2 distribute-list ACL
redistribute isis level-2 into level-1 distribute-list ACL
no redistribute isis level-1 into level-2
no redistribute isis level-2 into level-1
```

Parameter	Parameter Description	Parameter Value
level-1	Specify an inter-area route level-1.	-
level-2	Specify an inter-area routes level-2.	-
into	Specify a from level-n level into level-m.	-
distribute-list	Indicate the distributed-list parameter.	-
ACL	Access-list name	Up to 40 characters

Command Mode

Router Configuration

Address Family Configuration

Default

By default, redistributes selected level-1 routes into level-2

Usage

None

Examples

The following example shows how to redistributes level-2 routes into level-1:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# redistribute isis level-2 into level-1
```

Related Commands

None

6.8.53 router isis

Command Purpose

Use this command in global configuration mode to enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process. To disable IS-IS routing, use the no form of this command.

Use the no parameter with this command to disable IS-IS routing.

Command Syntax

```
router isis ( INSTANCE | )
no router isis ( INSTANCE | )
```

Parameter	Parameter Description	Parameter Value
INSTANCE	Specify an ISO routing instance tag.	Up to 20 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to set ISIS instance name and create it:

```
Switch# configure terminal
Switch(config)# router isis New
```

Related Commands

None

6.8.54 set-overload-bit

Command Purpose

To configure the router to signal other routers not to use it as an intermediate hop in their shortest path first (SPF) calculations, use the set-overload-bit command in router configuration mode. To remove the designation, use the noform of this command.

Command Syntax

```
set-overload-bit ( { suppress ( external | interlevel | external interlevel | interlevel external ) | on-startup ( TIME | wait-for-bgp ) } )
no set-overload-bit
```

Parameter	Parameter Description	Parameter Value
suppress	Specify to suppress specific types of IP prefixes.	-
external	Specify to redistribute external reachability (to prevent the IP prefixes learned from other protocols from being advertised).	-
interlevel	Specify to redistribute interlevel reachability.	-

Parameter	Parameter Description	Parameter Value
on-startup	Specify an interval in seconds after which the overload state is exited.	-
TIME	Specify the time in seconds to advertise one self as overloaded after reboot.	5-86400
wait-for-bgp	Specify that BGP determines when to unset the overload bit.	-

Command Mode

Router Configuration

Default

By default, no overload-bit is set.

Usage

None

Examples

The following example shows how to set overload bit:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# set-overload-bit
```

Related Commands

None

6.8.55 spf-interval-exp

Command Purpose

Use this command to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations.

The spf-interval-exp command configures the minimum and maximum interval time between the receipt of a topology change and the calculation of the SPF.

Use the no parameter with this command to set the minimum and maximum hold intervals to the default.

Command Syntax

```
spf-interval-exp EXP_MIN EXP_MAX
spf-interval-exp ( level-1 | level-2 ) <0-2147483647> <0-2147483647>
no spf-interval-exp
```

Parameter	Parameter Description	Parameter Value
EXP_MIN	Specify the minimum delay between receiving a change to the SPF calculation in milliseconds.	0-2147483647
EXP_MAX	Specify the maximum delay between receiving a change to the SPF calculation in milliseconds.	0-2147483647
level-1	Specify an interval for Level-1 IS.	-
level-2	Specify an interval for Level-2 IS.	-

Command Mode

Router Configuration

Default

By default, uses 500 milliseconds and 50,000 milliseconds for the minimum and maximum hold intervals, respectively. The values are applied to both level-1 and level-2 if the level parameter is omitted.

Usage

None

Examples

The following example shows how to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# spf-interval-exp level-1 600 60000
Switch(config-router)# no spf-interval-exp level-1
```

Related Commands

None

6.8.56 summary-address

Command Purpose

Use this command to configure Summary Address to summarize IPv4 reachability information.
Use the no parameter with this command to unconfigure the summary.

Command Syntax

```
summary-address IP_ADDR/IP_MASK_LEN ( level-1 | level-1-2 | level-2 | ) ( metric ) ( METRIC | )
no summary-address IP_ADDR/IP_MASK_LEN
```

Parameter	Parameter Description	Parameter Value
IP_ADDR/IP_MASK_LEN	Specify the IPv4 prefix to be announced.	IPv4 Address and mask length in A.B.C.D/M format
level-1	Specify the reachability information only for Level-1.	-
level-1-2	Specify the reachability information for both Level-1 and Level-2.	-
level-2	Specify the reachability information only for Level-2.	-
metric	Specify the metric for the summarized address.	-
METRIC	Specify the metric. The default is 0.	1-4294967295

Command Mode

Router Configuration

Default

By default, does not configure the summary-address. Summary-address is applied to Level-2 IS if level parameter is omitted.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to level-2

Examples

The following example shows how to configure ipv4 Summary Address:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# summary-address 10.10.0.0/16
```

Related Commands

None

6.8.57 summary-prefix

Command Purpose

Use this command to configure the summary prefix to summarize IPv6 reachability information.

Use the no parameter to unconfigure the summary.

Command Syntax

summary-prefix *GLOBAL_PREFIX/IPv6_MASK_LEN* (*level-1* | *level-1-2* | *level-2* |) (*metric METRIC*)

no summary-prefix *GLOBAL_PREFIX/IPv6_MASK_LEN*

Parameter	Parameter Description	Parameter Value
GLOBAL_PREFIX/IPv6_MASK_LEN	Specify the IPv6 prefix to be announced.	IPv4 Address and mask length in X:X::X/M format
level-1	Specify the reachability information only for Level-1.	-
level-1-2	Specify the reachability information for both Level-1 and Level-2.	-
level-2	Specify the reachability information only for Level-2.	-
metric	Specify the metric for the summarized address.	-
METRIC	Specify the metric. The default is 0.	1-4294967295

Command Mode

Address Family Configuration

Default

By default, does not configure the summary-prefix. Summary-prefix is applied to Level-2 IS if level parameter is omitted.

Usage

If neither the level-1 nor the level-2 keyword is configured, it applies to level-2

Examples

The following example shows how to configure ipv6 Summary Prefix:

```
Switch# configure terminal
Switch(config)# router isis bb
Switch(config-router)# address-family ipv6
Switch(config-router-af)# summary-prefix 3ffe:1234::/32
```

Related Commands

None

6.8.58 show clns is-neighbors

Command Purpose

Use this command to display all IS neighbor adjacencies.

Command Syntax

show clns is-neighbors (detail |)

show clns *INSTANCE* is-neighbors (detail |)

show clns is-neighbors *IFNAME* (detail |)

show clns *INSTANCE* is-neighbors *IFNAME* (detail |)

Parameter	Parameter Description	Parameter Value
INSTANCE	Display information for specified instance.	Up to 20 characters
IFNAME	Display information about a single interface.	Support physical/aggregation/loopback/vlan/tunnel ports
detail	Display detailed information for all interfaces.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display all IS neighbor adjacencies:

```
Switch# show clns is-neighbors
```

Area 100:

System Id	Interface	State	Type	Priority	Circuit Id
0000.0000.0002	vlan100	Up	L2	64	0000.0000.0001.01
0000.0000.0002	vlan200	Up	L2	64	0000.0000.0001.02

Related Commands

None

6.8.59 show debugging isis

Command Purpose

Use this command to display the status of the debugging of the ISIS system.

Command Syntax

```
show debugging isis
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the status of the debugging of the ISIS system:

```
Switch# show debugging isis
```

```
IS-IS debugging status:
```

```
IS-IS spf debugging is on
```

Related Commands

None

6.8.60 show ip isis route

Command Purpose

Use this command to display IS-IS routing table for IPv4.

Command Syntax

```
show ip isis ( INSTANCE | ) route
```

Parameter	Parameter Description	Parameter Value
INSTANCE	Display information for specified instance.	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display IS-IS routing table for IPv4.:

```
Switch# show ip isis route
```

Related Commands

None

6.8.61 show ipv6 isis route**Command Purpose**

Use this command to display the IS-IS routing table for IPv6.

Command Syntax

```
show ipv6 isis ( INSTANCE | ) route
```

Parameter	Parameter Description	Parameter Value
INSTANCE	Display information for specified instance.	Up to 20 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display IS-IS routing table for IPv6.:

```
Switch# show ipv6 isis route
```

Related Commands

None

6.8.62 show ipv6 isis topology

Command Purpose

Use this command to display the IS-IS topology for IPv6.

Command Syntax

show ipv6 isis topology (I1 | I2 | level-1 | level-2 |)

show ipv6 isis *INSTANCE* topology (I1 | I2 | level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
INSTANCE	Display information for specified instance.	Up to 20 characters
I1	IS-IS level-1 SPF topology.	-
I2	IS-IS level-2 SPF topology.	-
level-1	IS-IS level-1 SPF topology.	-
level-2	IS-IS level-2 SPF topology.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the IS-IS topology for IPv6:

```
Switch# show ipv6 isis topology
```

Related Commands

None

6.8.63 show ipv6 protocols isis

Command Purpose

Use this command to display IPv6 process parameters and statistics.

Command Syntax

```
show ipv6 protocols isis
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display IPv6 process parameters and statistics.:

```
Switch# show ipv6 protocols isis
```

```
Routing Protocol is "isis 2 "
```

```
  Redistributing:
```

```
    Area Address(es):
```

```
Distance : (default is 115)
```

```
Routing Protocol is "isis 1 "
```

```
  Redistributing:
```

```
    Area Address(es):
```

Distance : (default is 115)

Related Commands

None

6.8.64 show isis counter

Command Purpose

Use this command to display the IS-IS system counter entry MIBs.

Command Syntax

show isis counter

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the IS-IS system counter entry MIBs.:

```
Switch# show isis counter
```

```
Area b:
```

```
IS-IS Level-1 isisSystemCounterEntry:
```

```
isisSysStatCorrLSPs: 0
```

```
isisSysStatAuthTypeFails: 0
```

```
isisSysStatAuthFails: 0
```

```
isisSysStatLSPDbaseOloads: 0
```

```
isisSysStatManAddrDropFromAreas: 0
```

```
isisSysStatAttmptToExMaxSeqNums: 0
```

```
isisSysStatSeqNumSkips: 0
```

```
isisSysStatOwnLSPPurges: 0
```

```
isisSysStatIDFieldLenMismatches: 0
```

```
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 0
isisSysStatPRCRuns: 0
```

Area bb:

IS-IS Level-1 isisSystemCounterEntry:

```
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 0
isisSysStatPRCRuns: 0
```

IS-IS Level-2 isisSystemCounterEntry:

```
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 0
isisSysStatPRCRuns: 0
```

Related Commands

None

6.8.65 show isis database

Command Purpose

Use this command to display detailed link state database information.

Command Syntax

show isis database

show isis database (l1 | l2 | level-1 | level-2) *LSPID* (detail | verbose)

Parameter	Parameter Description	Parameter Value
detail	IS-IS link state database detailed information.	-
verbose	IS-IS link state database detailed information.	-
LSPID	LSPID in the form of XXXX.XXXX.XXXX.XX-XX.	-
l1	IS-IS level-1 link state database.	-
l2	IS-IS level-2 link state database.	-
level-1	IS-IS level-1 link state database.	-
level-2	IS-IS level-2 link state database.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display detailed link state database information.:

```
Switch# show isis database verbose
```

Area (null):

IS-IS Level-1 Link State Database:

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
0000.0000.0001.00-00*	0x00000002	0x9E50	1140	0/0/0

IS-IS Level-2 Link State Database:

LSPID	LSP Seq Num	LSP Checksum	LSP Holdtime	ATT/P/OL
0000.0000.0001.00-00*	0x00000003	0x9C51	1176	0/0/0

Related Commands

None

6.8.66 show isis interface

Command Purpose

Use this command to display detailed interface information.

Command Syntax

show isis interface

show isis interface *IFNAME*

show isis interface counter

Parameter	Parameter Description	Parameter Value
IFNAME	Display the name of interface.	Support physical/aggregation/loopback/vlan/tunnel ports
counter	Display the interface counters.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display detailed interface information about ISIS:

```
Switch# show isis interface eth-0-1
```

```
eth-0-1 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: e6f5.41de.3200
IP interface address:
  1.1.1.1/24
IPv6 interface address:
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
Number of active level-1 adjacencies: 0
Level-1 LSP MTU: 1492
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
Number of active level-2 adjacencies: 0
Level-2 LSP MTU: 1492
Next IS-IS LAN Level-1 Hello in 238 milliseconds
Next IS-IS LAN Level-2 Hello in 238 milliseconds
```

Related Commands

None

6.8.67 show isis topology

Command Purpose

Use this command to display data about IS-IS topology.

Command Syntax

show isis topology (I1 | I2 | level-1 | level-2 |)

show isis *INSTANCE* topology (I1 | I2 | level-1 | level-2 |)

Parameter	Parameter Description	Parameter Value
INSTANCE	Display information for specified instance.	Up to 20 characters
I1	Display the path to all level-1 routers in the area.	-
I2	Display the path to all level-2 routers in the domain.	-
level-1	Display the path to all level-1 routers in the area.	-
level-2	Display the path to all level-2 routers in the domain.	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display data about IS-IS topology.:

```
Switch# show isis topology
```

Related Commands

None

6.8.68 show running-config interface isis

Command Purpose

Use this command to display the ISIS interface configurations.

Command Syntax

show running-config interface IFNAME isis

Parameter	Parameter Description	Parameter Value
IFNAME	Display the name of interface.	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display the ISIS interface configurations.:

```
Switch# show running-config interface eth-0-1 isis
```

```
Building configuration...
```

```
!  
interface eth-0-1  
 ip router isis  
!
```

Related Commands

None

6.8.69 show running-config router isis

Command Purpose

Use this command to display router ISIS configurations.

Command Syntax

```
show running-config router isis
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display router ISIS configurations.:

```
Switch# show running-config router isis
```

```
Building configuration...
```

```
!  
router isis  
 net 10.0000.0000.0001.00  
!
```

Related Commands

None

Chapter 7 IPv6 Routing Commands

7.1 OSPFv3 Commands

7.1.1 area default-cost

Command Purpose

To specify a cost for the default summary route sent into a stub, use the area default-cost command in router configuration mode. To remove the assigned default route cost, use the no form of this command.

Command Syntax

area *AREA-ID* default-cost *COST*
no area *AREA-ID* default-cost

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
COST	Cost for the default summary route used for a stub.	0-16777215

Command Mode

Router Configuration

Default

The cost value is 1 by default.

Usage

The command is used only on an Area Border Router (ABR) attached to a stub. There are two stub area router configuration commands: the stub and default-cost options of the area command. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the stub option of the area command. Use the default-cost option only on an ABR attached to the stub area. The default-cost option provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
Switch# configure terminal
Switch(config)#router ipv6 ospf 201
Switch(config-router)#area 10.0.0.0 stub
Switch(config-router)#area 10.0.0.0 default-cost 20
```

Related Commands

None

7.1.2 area range

Command Purpose

To consolidate and summarize routes at an area boundary, use the area range command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

area *AREA-ID* range *ADDRESS/PREFIX-LENGTH* (advertise | not-advertise |)
no area *AREA-ID* range *ADDRESS/PREFIX-LENGTH*

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295
ADDRESS	IPv6 address	IPv6 Address
PREFIX-LENGTH	Prefix length of the address	1-128
advertise	Advertise this range (default)	-
not-advertise	Do Not Advertise this range	-

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The area range command is used only with Area Border Routers (ABRs). It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization. Multiple area router configuration commands specifying the range option can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on area 10:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 201
Switch(config-router)#area 10 range 2004::1/16
```

Related Commands

None

7.1.3 area stub

Command Purpose

To define an area as a stub area, use the area stub command in router configuration mode. To disable this function, use the no form of this command.

Command Syntax

```
area AREA-ID stub ( no-summary | )
no area AREA-ID stub ( no-summary | )
```

Parameter	Parameter Description	Parameter Value
AREA-ID	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address	IP address or number in the range of 0-4294967295

Parameter	Parameter Description	Parameter Value
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area	-

Command Mode

Router Configuration

Default

No stub area is defined.

Usage

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal router sent into a stub area by an ABR.

There are two stub area router configuration commands: the stub and default-cost options of the area router configuration command. In all routers attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Examples

The following example assigns a default cost of 20 to stub network 10.0.0.0:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 201
Switch(config-router)#area 10.0.0.0 stub
Switch(config-router)#area 10.0.0.0 default-cost 20
```

Related Commands

None

7.1.4 auto-cost

Command Purpose

To control how Open Shortest Path First Version 3 (OSPFv3) calculates default metrics for the interface; use the auto-cost command in router configuration mode.

To assign cost based only on the interface type, use the no form of this command.

Command Syntax

auto-cost reference-bandwidth *RATE*
no auto-cost reference-bandwidth

Parameter	Parameter Description	Parameter Value
RATE	Rate in Mbps (bandwidth). The default is 100	1 - 4294967 Mbps

Command Mode

Router Configuration

Default

100 Mbps

Usage

The value set by the ipv6 ospf cost command overrides the cost resulting from the auto-cost command.

Examples

The following example changes the cost of the cost link to 1GBps:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)#auto-cost reference-bandwidth 1000
```

Related Commands

ipv6 ospf cost

7.1.5 clear ipv6 ospf

Command Purpose

To clear routing information based on the Open Shortest Path First (OSPF) routing process ID, use the clear ipv6 ospf command in privileged EXEC mode.

Command Syntax

clear ipv6 ospf (*PID* |) process

Parameter	Parameter Description	Parameter Value
PID	(Optional) Process ID	0-65535

Command Mode

Privileged EXEC

Default

None

Usage

Use the PID argument to clear only one OSPFv3 process. If the PID argument is not specified, all OSPFv3 processes are cleared.

Examples

The following example clears all OSPFv3 processes:

```
Switch# clear ipv6 ospf process
```

Related Commands

None

7.1.6 default-information originate (OSPFv3)

Command Purpose

To generate a default external route into an Open Shortest Path First Version3 (OSPFv3) routing domain, use the default-information originate command in router configuration mode.

To disable this feature, use the no form of this command.

Command Syntax

```
default-information originate
default-information originate { metric METRIC | metric-type TYPE } | route-map ROUTE_MAP | always }
no default-information originate
no default-information originate { metric | metric-type | route-map | always }
```

Parameter	Parameter Description	Parameter Value
always	(Optional) Always advertises the default route regardless of whether the system has a default route	Up to 20 characters

Parameter	Parameter Description	Parameter Value
METRIC	metric-value (Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the default-metric router configuration command, the default metric value is 10. The value used is specific to the protocol	0-16777214
TYPE	(Optional) External link type associated with the default route advertised into the OSPF routing domain. It can be one of the following values	1,2
ROUTE_MAP	Route map reference	-

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPFv3 routing domain, the switch automatically becomes an autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPFv3 routing domain. The system still must have a default route for itself before it generates one, except when you have specified the always keyword.

Examples

The following example specifies a metric of 100 for the default route redistributed into the OSPFv3 routing domain and an external metric type of Type 1:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 109
Switch(config-router)# redistribute rip metric 100
Switch(config-router)#default-information originate metric 100 metric-type 1
```

Related Commands

redistribute (OSPFv3)

7.1.7 default-metric (OSPFv3)

Command Purpose

To set default metric values for the Open Shortest Path First Version3 (OSPFv3) routing protocol, use the default-metric command in router configuration mode.

To return to the default state, use the no form of this command.

Command Syntax

```
default-metric METRIC-VALUE
no default-metric ( METRIC-VALUE )
```

Parameter	Parameter Description	Parameter Value
METRIC-VALUE	Default metric value appropriate for the specified routing protocol.	
	Default metric value appropriate for the specified routing protocol.	
	Built-in, automatic metric translations, as appropriate for each routing protocol. The metric of redistributed connected and static routes is set to 0	0-16777214

Command Mode

Router Configuration

Default

default-metric is 20

Usage

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a router in autonomous system using both the Routing Information Protocol (RIPng) and the OSPFv3 routing protocols. The example advertises OSPFv3-derived routes using RIPng and assigns the Internal Gateway Protocol (IGP)-derived routes a RIPng metric of 10:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute ripng
```

Related Commands

redistribute (OSPFv3)

7.1.8 distance (OSPFv3)

Command Purpose

To define Open Shortest Path First Version3 (OSPFv3) route administrative distances based on route type, use the distance command in router configuration mode.

To restore the default value, use the no form of this command.

Command Syntax

```
distance { DISTANCE | ospfv3 [ external DIST1 ] [ inter-area DIST2 ] [ intra-area DIST3 ] }
no distance { DISTANCE | ospfv3 }
```

Parameter	Parameter Description	Parameter Value
DISTANCE	Administrative distance.	1-254.(routes with a distance value of 255 are not installed in the routing table)

Parameter	Parameter Description	Parameter Value
external DIST1	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. Range is 1 to 255. The default value is 110	1-254
inter-area DIST2	(Optional) Sets the distance for all routes from one area to another area. Range is 1 to 255. The default value is 110	1-254
intra-area DIST3	(Optional) Sets the distance for all routes within an area. Range is 1 to 255. The default value is 110	1-254

Command Mode

Router Configuration

Default

DIST1: 110
DIST2: 110
DIST3: 110

Usage

You may specify one of the keywords or use distance only to apply to all types of routes. The distance command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list. A common reason to use the distance command is when you have multiple OSPFv3 processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Examples

The following example shows a router in autonomous system using both the Routing Information Protocol (RIPng) and the OSPFv3 routing protocols. The example advertises OSPFv3-derived routes using RIPng and assigns the Internal Gateway Protocol (IGP)-derived routes a RIPng distance of 90:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# distance 90
Switch(config-router)# redistribute ripng
```

Related Commands

None

7.1.9 distribute-list (OSPFv3)

Command Purpose

To filter networks received in updates or suppress networks from being advertised in updates, use the distribute-list command in router configuration mode.

To cancel this function, use the no form of this command.

Command Syntax

```
distribute-list ACCESSS-LIST-NAME ( in | out ( bgp | connected | ospfv3 | ripng | static ) )
no distribute-list ACCESSS-LIST-NAME ( in | out ( bgp | connected | ospfv3 | ripng | static ) )
```

Parameter	Parameter Description	Parameter Value
ACCESSS-LIST-NAME	Name of an access list to be applied	Up to 20 characters
in	Filter networks received in updates	-

Parameter	Parameter Description	Parameter Value
out	Suppress networks from being advertised in updates	-

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

This command must specify an access list.

Examples

In the following example, OSPFv3 process 1 is configured to accept two prefixes, prefix 2001:1:1::1/32 and prefix 3001:1:1::1/32:

```
Switch# configure terminal
Switch(config)# ipv6 access-list filter-as-router
Switch(config-ip-acl)# permit any 2001:1:1::1/32 any
Switch(config-ip-acl)# permit any 3001:1:1::1/32 any
Switch(config-ip-acl)# deny any any any
Switch(config)# router ipv6 ospf 1
Switch(config-router)# distribute-list acl1 in
```

Related Commands

ipv6 access-list

7.1.10 enable db-summary-opt**Command Purpose**

Use this command to enable optimize the process when building ospfv3 neighbor ship.

Command Syntax

```
enable db-summary-opt
no enable db-summary-opt
```

Command Mode

Router Configuration

Default

Disable

Usage

After this function enabled, if the router receives a DD packet which has newer LSA, the router should delete the LSA in the database summary list, and should not send this LSA to its neighbor.

Examples

The following example enables this optimization:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-if)# enable db-summary-opt
```

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)# enable db-summary-opt
```

Related Commands

None

7.1.11 ipv6 ospf cost

Command Purpose

To explicitly specify the cost of sending a packet on an interface, use the `ipv6 ospf cost` command in interface configuration mode. To reset the path cost to the default value, use the `no` form of this command.

Command Syntax

```
ipv6 ospf cost INTERFACE-COST ( instance ID | )  
no ipv6 ospf cost ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
INTERFACE-COST	Unsigned integer value expressed as the link-state metric.	1-65535

Command Mode

Interface Configuration

Default

No default cost is predefined.

Usage

You can set the metric manually using this command, if you need to change the default. Using the `bandwidth` command changes the link cost as long as this command is not used.

The link-state metric is advertised as the link cost in the router link advertisement.

In general, the path cost is calculated using the following formula:

Reference Bandwidth / bandwidth

Examples

The following example sets the interface cost value to 65:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# no switchport  
Switch(config-if)# ipv6 ospf cost 65
```

Related Commands

`auto-cost reference bandwidth`

7.1.12 ipv6 ospf dead-interval

Command Purpose

To set the interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down, use the `ipv6 ospf dead-interval` command in interface configuration mode. To restore the default value, use the `no` form of this command.

Command Syntax

```
ipv6 ospf dead-interval SECONDS ( instance ID | )  
no ipv6 ospf dead-interval ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
SECONDS	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The value must be the same for all nodes on the network	1-65535
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

The neighbor is considered as dead in 40s by default.

Usage

The dead interval is advertised in OSPFv3 hello packets. This value must be the same for all networking devices on a specific network. Specifying a smaller dead interval (seconds) will give faster detection of a neighbor being down and improve convergence, but might cause more routing instability.

Examples

The following example sets the OSPFv3 dead interval to 20 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf dead-interval 20
```

Related Commands

```
ipv6 ospf hello-interval
show ipv6s ospf interface
```

7.1.13 ipv6 ospf hello-interval

Command Purpose

To specify the interval between hello packets that the switch sends on the interface, use the `ip ospf hello-interval` command in interface configuration mode.

To return to the default time, use the `no` form of this command.

Command Syntax

```
ip ospf hello-interval SECONDS ( instance ID | )
no ip ospf hello-interval ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
SECONDS	Interval (in seconds) during which the router must receive at least one hello packet from a neighbor or else that neighbor is removed from the peer list and does not participate in routing. The value must be the same for all nodes on the network	1-65535
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

10 seconds (Ethernet)
30 seconds (non-broadcast)

Usage

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the interval between hello packets to 15 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf hello-interval 15
```

Related Commands

ipv6 ospf dead-interval

7.1.14 ipv6 ospf mtu-ignore

Command Purpose

To disable Open Shortest Path First Version3 (OSPFv3) maximum transmission unit (MTU) mismatch detection on receiving Database Descriptor (DBD) packets, use the `ipv6 ospf mtu-ignore` command in interface configuration mode. To reset to default, use the `no` form of this command.

Command Syntax

```
ipv6 ospf mtu-ignore ( instance ID | )
no ipv6 ospf mtu-ignore ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

OSPFv3 MTU mismatch detection is enabled.

Usage

OSPFv3 checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPFv3 adjacency will not be established.

Examples

The following example disables MTU mismatch detection on receiving DBD packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf mtu-ignore
```

Related Commands

None

7.1.15 ipv6 ospf priority

Command Purpose

To set the router priority, which helps determine the designated router for this network, use the `ip ospf priority` command in interface configuration mode.

To return to the default value, use the `no` form of this command.

Command Syntax

```
ipv6 ospf priority NUMBER-VALUE ( instance ID | )
no ipv6 ospf priority ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	A number value that specifies the priority of the router.	0-255
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

Priority of 1

Usage

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multi-access networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First Version3 (OSPFv3) for non-broadcast networks using the neighbor router configuration command for OSPFv3.

Examples

The following example sets the router priority value to 4:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf priority 4
```

Related Commands

None

7.1.16 ipv6 ospf retransmit-interval

Command Purpose

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the `ipv6 ospf retransmit-interval` command in interface configuration mode. To return to the default value, use the `no` form of this command.

Command Syntax

```
ipv6 ospf retransmit-interval SECONDS ( instance ID | )  
no ipv6 ospf retransmit-interval ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network.	1-65535 seconds
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

5 seconds

Usage

When a router sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the router receives no acknowledgment, it will resend the LSA. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example sets the retransmit interval value to 8 seconds:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# no switchport  
Switch(config-if)# ipv6 ospf retransmit-interval 8
```

Related Commands

None

7.1.17 ipv6 ospf transmit-delay

Command Purpose

To set the estimated time required to send a link-state update packet on the interface, use the `ipv6 ospf transmit-delay` command in interface configuration mode. To return to the default value, use the `no` form of this command.

Command Syntax

```
ipv6 ospf transmit-delay SECONDS ( instance ID | )  
no ipv6 ospf transmit-delay ( instance ID | )
```

Parameter	Parameter Description	Parameter Value
SECONDS	Time (in seconds) between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network.	1-65535 seconds
ID	Instance ID, the default value is 0.	0-255

Command Mode

Interface Configuration

Default

1 second

Usage

Link-state advertisements (LSAs) in the update packet must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the retransmit delay value to 3 seconds:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 ospf transmit-delay 3
```

Related Commands

None

7.1.18 passive-interface (OSPF)

Command Purpose

To disable sending routing updates for the Open Shortest Path First Version3 (OSPFv3) on an interface, use the passive-interface command in router configuration mode. To re-enable the sending of routing updates, use the no form of this command.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

Parameter	Parameter Description	Parameter Value
		Support
IFNAME	The interface name	physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

Routing updates are sent on the interface.

Usage

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other switches on that interface continue to be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 200
Switch(config-router)# passive-interface eth-0-1
```

Related Commands

router ipv6 ospf

7.1.19 redistribute (OSPFv3)

Command Purpose

To redistribute routes from one routing domain into Open Shortest Path First Version3 (OSPFv3) routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax

redistribute *PROTOCOL* [route-map *WORD*] [tag *TAG-VALUE*] [metric *METRIC-VALUE*] [metric-type *TYPE-VALUE*]
no redistribute *PROTOCOL* [metric *METRIC -VALUE*] [metric-type *TYPE-VALUE*]

Parameter	Parameter Description	Parameter Value
route-map WORD	Route map name	Up to 20 characters
PROTOCOL	(Optional) The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol, use one of the following keywords: bgp, and ripng	connected/static/bgp/ripng
tag TAG-VALUE	Set tag for routes redistributed into OSPF	0-4294967295
metric METRIC-VALUE	(Optional) When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified	0-16777214
metric-type TYPE-VALUE	For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values	1-2

Command Mode

Router Configuration

Default

Route redistribution is disabled.
metric metric-value: 20
metric-type TYPE-VALUE: Type 2 external route

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples

The following example redistribute the static routes into OSPFv3 with metric 10:

```
Switch# configure terminal
Switch(config)# router ospf 119
Switch(config-router)# redistribute static metric 10
```

Related Commands

default-metric

7.1.20 router-id (OSPF)

Command Purpose

To use a fixed router ID, use the router-id command in router configuration mode.

To force Open Shortest Path First Version3 (OSPFv3) use the previous OSPF router ID behavior, use the no form of this command.

Command Syntax

```
router-id IP-ADDRESS
no router-id
```

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	Router ID in IP address format	IPv6 Address

Command Mode

Router Configuration

Default

No OSPF routing process is defined.

Usage

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If this command is used on an OSPFv3 router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPFv3 process restart. To manually restart the OSPFv3 process, use the clear ip ospf command.

Examples

The following example specifies a fixed router-id:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 119
Switch(config-router)# router-id 10.1.1.1
```

Related Commands

```
clear ipv6 ospf
router ipv6 ospf
```

7.1.21 router ipv6 ospf

Command Purpose

To configure an Open Shortest Path First Version3 (OSPFv3) routing process, use the router ipv6 ospf command in global configuration mode. To terminate an OSPFv3s routing process, use the no form of this command.

Command Syntax

```
router ipv6 ospf [ PROCESS-ID ]
no router ipv6 ospf [ PROCESS-ID ]
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process	1-65535

Command Mode

Global Configuration

Default

No OSPF routing process is defined.

Usage

You can specify multiple OSPFv3 routing processes in each router. If you do not specify the process-id, the process-id will be the default 0.

Examples

The following example configures an OSPFv3 routing process and assigns a process number of 109:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 109
```

Related Commands

None

7.1.22 summary-address (OSPFv3)

Command Purpose

To create aggregate addresses for Open Shortest Path First Version3 (OSPFv3), use the summary-address command in router configuration mode. To restore the default, use the no form of this command.

Command Syntax

```
summary-address PREFIX / PREFIX-LENGTH [ not-advertise ] [ tag TAG-VALUE ]
no summary-address PREFIX / PREFIX-LENGTH [ not-advertise ] [ tag TAG-VALUE ]
```

Parameter	Parameter Description	Parameter Value	
PREFIX	IP route prefix for the destination	IPv6 Address	
PREFIX-LENGTH	Prefix length for the network	1-128	
not-advertise	(Optional) Suppress routes that match the specified prefix/mask pair. This keyword applies to OSPFv3 only	-	
tag TAG-VALUE	Route tag value	0-4294967295	

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the largest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPFv3 causes an OSPFv3 Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPFv3, this command summarizes only routes from other routing protocols that are being redistributed into OSPFv3. Use the area range command for route summarization between OSPF areas. OSPFv3 does not support the summary-address 0.0.0.0/0 command.

Examples

In the following example, the summary address 2001:1:1::/48 includes address 2001:1:1:1::/64, 2001:1:1:2::/64, and so on. Only the address 2001:1:1:1::/48 is advertised in an external link-state advertisement:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf
Switch(config-router)# summary-address 2001:1:1::/48
```

Related Commands

area range

7.1.23 show ipv6 ospf

Command Purpose

To display general information about Open Shortest Path First Version3 (OSPFv3) routing processes, use the show ipv6 ospf command in user EXEC or privileged EXEC mode.

Command Syntax

show ipv6 ospf (*PROCESS-ID* |)

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPFv3 routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPFv3 routing process	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ipv6 ospf command when entered without a specific OSPFv3 process ID:
Switch# show ipv6 ospf 65535

```
Routing Process "OSPFv3 (65535)" with ID 1.1.1.1
  Process uptime is 1 hour 52 minutes
  SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 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 3
  Number of LSA received 19
  Number of areas in this router is 1
    Area BACKBONE(0)
      Number of interfaces in this area is 1(1)
      SPF algorithm executed 6 times
      Number of LSA 4. Checksum Sum 0x16569
      Number of Unknown LSA 0
```

Related Commands

None

7.1.24 show ipv6 ospf database

Command Purpose

To display lists of information related to the Open Shortest Path First Version3 (OSPFv3) database for a specific router, use the show ip ospf database command in EXEC mode.

Command Syntax

```

show ipv6 ospf ( PROCESS-ID | ) database
show ipv6 ospf ( PROCESS-ID | ) database adv-router ROUTER-ID
show ipv6 ospf ( PROCESS-ID | ) database ( external | inter-prefix | inter-router | intra-prefix | link | network | router ) ( LINK-STATE-ID | )
( adv-router ROUTER-ID | self-originate )
show ipv6 ospf ( PROCESS-ID | ) database max-age
show ipv6 ospf ( PROCESS-ID | ) database self-originate

```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	Internally used identification parameter for an OSPFv3 routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPFv3 routing process	1-65535
adv-router ROUTER-ID	(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate)	IPv4 Address in A.B.C.D format
LINK-STATE-ID	(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address	IPv4 Address in A.B.C.D format

Command Mode

Privileged EXEC

Default

None

Usage

The various forms of this command deliver information about different OSPFv3 link state advertisements.

Examples

The following is sample output from the show ipv6 ospf database command when no arguments or keywords are used:
Switch# show ipv6 ospf 65535 database

```

OSPFv3 Router with ID (1.1.1.1) (Process 65535)
  Link-LSA (Interface vlan1000)
Link State ID  ADV Router    Age  Seq#           CkSum  Prefix
0.0.19.232    1.1.1.1      1492 0x800000002 0x27e3    1
0.0.19.232    2.2.2.2      1488 0x800000002 0xcc94    1
  Router-LSA (Area 0.0.0.0)
Link State ID  ADV Router    Age  Seq#           CkSum  Link
0.0.0.0       1.1.1.1      1452 0x800000003 0x42d6    1
0.0.0.0       2.2.2.2      1449 0x800000003 0x24f0    1
  Network-LSA (Area 0.0.0.0)
Link State ID  ADV Router    Age  Seq#           CkSum
0.0.19.232    2.2.2.2      1453 0x800000001 0x7f99
  Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID  ADV Router    Age  Seq#           CkSum  Prefix  Reference
0.0.0.2       2.2.2.2      1448 0x800000001 0x96fd    2  Network-LSA

```

Related Commands

None

7.1.25 show ipv6 ospf interface

Command Purpose

To display Open Shortest Path First Version3 (OSPFv3)-related interface information; use the show ipv6 ospf interface command in EXEC mode.

Command Syntax

show ipv6 ospf interface (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output of the show ipv6 ospf interface command when vlan12 is specified:

Switch# show ipv6 ospf interface vlan 12

```
vlan12 is up, line protocol is up
Interface ID 4108
IPv6 Prefixes
 fe80::8eb5:d5ff:fed9:ff00/10 (Link-Local Address)
 2004:12:0:12::1/96
OSPFv3 Process (0), Area 0.0.0.0, Instance ID 0
 Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State Backup, Priority 1
 Designated Router (ID) 2.2.2.2
  Interface Address fe80::188f:beff:fe99:9800
 Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::8eb5:d5ff:fed9:ff00
 Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:06
 Neighbor Count is 1, Adjacent neighbor count is 1
```

Related Commands

None

7.1.26 show ipv6 ospf neighbor

Command Purpose

To display Open Shortest Path First Version3 (OSPFv3)-neighbor information on a per-interface basis, use the show ipv6 ospf neighbor command in privileged EXEC mode.

Command Syntax

show ipv6 ospf neighbor (*IFNAME* |) (*NEIGHBOR-ID* |) (detail |)

Parameter	Parameter Description	Parameter Value
IFNAME	(Optional) Interface name. If the interface-name argument is included, only information for the specified interface is included	Support physical/aggregation/loopback/vlan/tunnel ports
NEIGHBOR-ID	(Optional) Neighbor ID	IPv4 Address in A.B.C.D format
detail	(Optional) Displays all neighbors given in detail (lists all neighbors)	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ipv6 ospf neighbor command showing a single line of summary information for each neighbor:

```
Switch# show ipv6 ospf neighbor
```

```
OSPFv3 Process (0)
Neighbor ID  Pri  State      Dead Time  Interface  Instance ID
2.2.2.2      1    Full/DR    00:00:31   vlan12     0
2.2.2.2      1    Full/DR    00:00:33   vlan1212   0
OSPFv3 Process (65535)
Neighbor ID  Pri  State      Dead Time  Interface  Instance ID
2.2.2.2      1    Full/DR    00:00:31   vlan1000   0
```

Related Commands

None

7.1.27 show ipv6 ospf database database-summary**Command Purpose**

To display the summary of database used by OSPFv3, use the show ip ospf database database-summary command in privileged EXEC mode.

Command Syntax

```
show ipv6 ospf ( PROCESS-ID | ) database database-summary
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ipv6 ospf database database-summary command:

```
Switch# show ipv6 ospf 65535 database database-summary
```

```
          OSPFv3 Router with ID (1.1.1.1) (Process ID 65535)
Area (0.0.0.0) database summary
 LSA Type          Count          MaxAge
Router              2              0
Network            1              0
Inter-Prefix       0              0
Inter-Router       0              0
Intra-Prefix       1              0
Subtotal           4              0
Process 65535 database summary
 LSA Type          Count          MaxAge
Router              2              0
Network            1              0
Inter-Prefix       0              0
Inter-Router       0              0
Type-5 Ext         0              0
Link               2              0
Intra-Prefix       1              0
Total              6              0
```

Related Commands

None

7.1.28 show ipv6 ospf route**Command Purpose**

To display the summary of routes used by OSPFv3, use the show ipv6 ospf route summary command in privileged EXEC mode.

Command Syntax

```
show ipv6 ospf ( PROCESS-ID | ) route
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ipv6 ospf route command:

```
Switch# show ipv6 ospf route
```

```
OSPFv3 Process (0)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
      E1 - OSPF external type 1, E2 - OSPF external type 2
      Destination                                Metric
      Next-hop
C 2004:1:0:10::/96                               1
  directly connected, vlan10, Area 0.0.0.0
C 2004:1:0:20::/96                               1
  directly connected, vlan20, Area 0.0.0.14
C 2004:1:0:100::/96                             1
  directly connected, vlan100, Area 0.0.0.0
C 2004:1:0:200::/96                             1
  directly connected, vlan200, Area 0.0.0.14
O 2004:2:0:10::/96                               2
  via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0
  via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0
IA 2004:2:0:20::/96                             2
  via fe80::188f:beff:fe99:9800, vlan1212, Area 0.0.0.0
  via fe80::188f:beff:fe99:9800, vlan12, Area 0.0.0.0
```

Related Commands

None

7.1.29 show ipv6 ospf route summary

Command Purpose

To display the summary of routes used by OSPFv3, use the show ipv6 ospf route summary command in privileged EXEC mode.

Command Syntax

```
show ipv6 ospf ( PROCESS-ID | ) route summary
```

Parameter	Parameter Description	Parameter Value
PROCESS-ID	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPFv3 routing process	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ipv6 ospf route summary command:

```
Switch# show ipv6 ospf route summary
```

```
OSPFv3 Router with ID (1.1.1.1) (Process ID 0)
Route Type      Count
(C)Connected    8
```

(D)Discard	0
(O)Intra area	2
(IA)Inter area	4
(E1)Ext type 1	0
(E2)Ext type 2	0
(N1)NSSA Ext type 1	0
(N2)NSSA Ext type 2	0
Total	14
OSPFv3 Router with ID (1.1.1.1) (Process ID 65535)	
Route Type	Count
(C)Connected	1
(D)Discard	0
(O)Intra area	1
(IA)Inter area	0
(E1)Ext type 1	0
(E2)Ext type 2	0
(N1)NSSA Ext type 1	0
(N2)NSSA Ext type 2	0
Total	2

Related Commands

None

7.1.30 show ipv6 protocols ospf

Command Purpose

To display IPv6 routing protocol process parameters and statistics of Open Shortest Path First Version3 (OSPFv3), use the show ipv6 ospf protocols ospf command in privileged EXEC mode.

Command Syntax

```
show ipv6 protocols ospf
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to use show ipv6 protocols ospf command:

```
Switch# show ipv6 protocols ospf
```

```
Routing Protocol is "OSPFv3 (0)" with ID 1.1.1.1
```

```
Redistributing:
```

```
Distance: (default is 110)
```

```
Routing Protocol is "OSPFv3 (65535)" with ID 1.1.1.1
```

```
Redistributing:
```

```
Distance: (default is 110)
```

Related Commands

None

7.1.31 timers spf

Command Purpose

To turn on Open Shortest Path First Version3 (OSPFv3) shortest path first (SPF) throttling, use the timers spf command in router configuration mode. To turn off SPF throttling, use the no form of this command.

Command Syntax

timers spf exp *SPF-HOLD_MIN* *SPF-HOLD_MAX*
no timers spf exp

Parameter	Parameter Description	Parameter Value
SPF-HOLD_MIN	Indicates the maximum hold time between two consecutive SPF calculations.	0-2147483647 milliseconds
SPF-HOLD_MAX	Indicates the minimum hold time between two consecutive SPF calculations.	0-2147483647 milliseconds

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example shows how to configure SPF calculation parameters:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 1
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# timers spf exp 20 50
```

Related Commands

None

7.1.32 max-concurrent-dd

Command Purpose

To specify Maximum number allowed to process DD concurrently, use the max-concurrent-dd command in router configuration mode. To restore default value, use the no form of this command

Command Syntax

max-concurrent-dd *NUMBER-VALUE*
no max-concurrent-dd

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Number of DD process	1-65535

Command Mode

Router Configuration

Default

None

Usage

This command used to specify Maximum number allowed to process DD concurrently.

Examples

The following example shows how to use max-concurrent-dd command:

```
Switch# configure terminal
Switch(config)# router ipv6 ospf 100
Switch(config-router)# router-id 10.10.10.2
Switch(config-router)# max-concurrent-dd 10
```

Related Commands

None

7.1.33 debug ipv6 ospf

Command Purpose

Use this command to specify all debugging options for OSPFv3. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf ( all | )
no debug ipv6 ospf ( all | )
```

Parameter	Parameter Description	Parameter Value
all	enable all debugging	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf all command enables the display of all debug information.

Examples

```
Switch# debug ipv6 ospf all
Switch# debug ipv6 ospf
```

Related Commands

None

7.1.34 debug ipv6 ospf events

Command Purpose

Use this command to specify debugging options for OSPFv3 event troubleshooting. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf events ( abr | asbr | nssa | os | router | vlink )
no debug ipv6 ospf events ( abr | asbr | nssa | os | router | vlink )
```

Parameter	Parameter Description	Parameter Value
abr	shows ABR events	-
asbr	shows ASBR events	-
nssa	shows NSSA events	-
os	shows OS interaction events	-
router	shows others router events	-

Parameter	Parameter Description	Parameter Value
vlink	shows virtual link events	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf event command enables the display of debug information related to OSPFv3 internal events.

Examples

```
Switch# debug ipv6 ospf events nssa  
Switch# debug ipv6 ospf events lsa
```

Related Commands

None

7.1.35 debug ipv6 ospf ifsm**Command Purpose**

Use this command to specify debugging options for OSPFv3 Interface Finite State Machine (IFSM) troubleshooting.
Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf ifsm ( status | events | timers )  
no debug ipv6 ospf ifsm ( status | events | timers )
```

Parameter	Parameter Description	Parameter Value
status	Displays IFSM status information	-
events	Displays IFSM event information	-
timers	Displays IFSM TIMER information	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf ifsm command enables the display of debug information related to the Interface Finite State Machine (IFSM).

Examples

```
Switch# debug ipv6 ospf ifsm timers
```

Related Commands

None

7.1.36 debug ipv6 ospf nfsm**Command Purpose**

Use this command to specify debugging options for OSPFv3 Neighbor Finite State Machine (NFSM) troubleshooting.

Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf nfsm ( status | events | timers )  
no debug ipv6 ospf nfsm ( status | events | timers )
```

Parameter	Parameter Description	Parameter Value
status	Displays NFSM status information	-
events	Displays NFSM event information	-
timers	Displays NFSM TIMER information	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf nfsm command enables the display of debug information related to the Neighbor Finite State Machine (NFSM).

Examples

```
Switch# debug ipv6 ospf nfsm timers
```

Related Commands

None

7.1.37 debug ipv6 ospf lsa

Command Purpose

Use this command to specify debugging options for OSPFv3 Link State Advertisements (LSA) troubleshooting.
Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf lsa ( flooding | generate | install | maxage | refresh )  
no debug ipv6 ospf lsa ( flooding | generate | install | maxage | refresh )
```

Parameter	Parameter Description	Parameter Value
flooding	Displays LSA flooding	-
generate	Displays LSA generate	-
install	Displays LSA installation	-
maxage	Displays the maximum age of LSA in seconds	-
refresh	Displays LSA refresh	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf lsa command enables the display of debug information related to internal operations of LSAs.

Examples

```
Switch# debug ipv6 ospf lsa install
```

Related Commands

None

7.1.38 debug ipv6 ospf packet

Command Purpose

Use this command to specify debugging options for OSPFv3 packets.
Use the no parameter with this command to disable this function..

Command Syntax

```
debug ipv6 ospf packet PARAMETERS  
no debug ipv6 ospf packet PARAMETERS  
PARAMETERS = dd | detail | hello | ls-ack | ls-request | ls-update | recv | send
```

Parameter	Parameter Description	Parameter Value
dd	Specifies debugging for OSPF database descriptions	-
detail	Sets the debug option to detailed information	-
hello	Specifies debugging for OSPF hello packets	-
ls-ack	Specifies debugging for OSPF link state acknowledgments	-
ls-request	Specifies debugging for OSPF link state requests	-
ls-update	Specifies debugging for OSPF link state updates	-
recv	Specifies the debug option set for received packets	-
send	Specifies the debug option set for sent packets	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf packet command enables the display of debug information related to the sending and receiving of packets.

Examples

```
Switch# debug ipv6 ospf packet dd send detail
```

Related Commands

None

7.1.39 debug ipv6 ospf route

Command Purpose

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options. Use the no parameter with this command to disable this function.

Command Syntax

```
debug ipv6 ospf route ( ase | ia | install | spf )  
no debug ipv6 ospf route ( ase | ia | install | spf )
```

Parameter	Parameter Description	Parameter Value
ase	Specifies the debugging of external route calculation	-
ia	Specifies the debugging of Inter-Area route calculation	-
install	Specifies the debugging of route installation	-
spf	Specifies the debugging of SPF calculation	-

Command Mode

Privileged EXEC

Default

None

Usage

The debug ospf route command enables the display of debug information related to route-calculation

Examples

```
Switch# debug ipv6 ospf route install
```

Related Commands

None

7.1.40 show debugging ipv6 ospf

Command Purpose

Use this command to display the set OSPFv3 debugging option..

Command Syntax

```
show debugging ipv6 ospf
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This is a sample output from the show debugging ipv6 ospf command. Some lines in this output wrap around, they might not wrap around in the actual display:

```
Switch# show debugging ipv6 ospf
```

```
OSPFv3 debugging status:
  OSPFv3 all packet detail debugging is on
  OSPFv3 all IFSM debugging is on
  OSPFv3 all NFSM debugging is on
  OSPFv3 all LSA debugging is on
  OSPFv3 all route calculation debugging is on
  OSPFv3 all event debugging is on
```

Related Commands

None

7.1.41 show resource ipv6 ospf

Command Purpose

Use this command to display the route resources used by OSPFv3 protocol.

Command Syntax

```
show resource ipv6 ospf
```

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following is sample output from the show resource ipv6 ospf command:

```
Switch# show resource ipv6 ospf
```

OSPFv3 Resource	Used	Capability
Routes	16	1913

Related Commands

```
show ipv6 ospf route summary
```

7.2 RIPng Commands

7.2.1 router ipv6 rip

Command Purpose

To enable or configure the Routing Information Protocol next generation (RIPng) routing process, use the router ipv6 rip command in global configuration mode.

To disable the RIPng routing process, use the no form of this command.

Command Syntax

```
router ipv6 rip
no router ipv6 rip
```

Command Mode

Global Configuration

Default

No RIPng routing process is defined.

Usage

None

Examples

The following example shows how to enable RIPng routing process:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
```

Related Commands

None

7.2.2 ipv6 router rip**Command Purpose**

To enable RIPng routing process on specific interface, use the command `ipv6 router rip` in interface configuration mode. Use the `no` parameter with this command to disable RIPng routing process on interface.

Command Syntax

```
ipv6 router rip
no ipv6 router rip
```

Command Mode

Interface Configuration

Default

None.

Usage

None

Examples

The following example shows how to enable RIPng on the interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 router rip
```

Related Commands

None

7.2.3 ipv6 rip metric-offset**Command Purpose**

Use this command to set RIP metric offset in interface mode. To restore the default metric, use the `no` form of this command.

Command Syntax

```
ipv6 rip metric-offset NUMBER-VALUE
no ipv6 rip metric-offset NUMBER-VALUE
```

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Metric offset value	1-16

Command Mode

Interface Configuration

Default

Metric offset value is 1.

Usage

Metric offset value is used to add the metric of the network on which the message arrived (as the RFC describes).

Examples

The following example shows how to set metric offset as 2:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 rip metric-offset 2
```

Related Commands

None

7.2.4 ipv6 rip split-horizon**Command Purpose**

To enable the split horizon mechanism for Routing Information Protocol next generation (RIPng), use the `ipv6 rip split-horizon` command in interface configuration mode.

To disable the split horizon mechanism, use the `no` form of this command.

Command Syntax

```
ipv6 rip split-horizon (poisoned | )
no ipv6 rip split-horizon
```

Parameter	Parameter Description	Parameter Value
poisoned	Split horizon with poisoned reverse	-

Command Mode

Interface Configuration

Default

This command is enabled with poisoned reverse by default.

Usage

In general, changing the default state for the `ipv6 rip split-horizon` command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes.

Examples

The following example enables split horizon without poisoned reverse:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 rip split-horizon
```

Related Commands

None

7.2.5 default-information originate (RIPng)

Command Purpose

To generate a default route into Routing Information Protocol next generation (RIPng), use the default-information originate command in router configuration mode.

To disable this feature, use the no form of this command.

Command Syntax

default-information originate (route-map *NAME* |)

no default-information originate

Parameter	Parameter Description	Parameter Value
NAME	Route map name to reference	Up to 20 characters

Command Mode

Router Configuration

Default

This command is disabled by default.

Usage

The default route can be learned by neighbor, but can't be stored in FIB.

Examples

The following example originates a default route (0::0/0) into RIPng:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# default-information originate
```

Related Commands

None

7.2.6 default-metric (RIPng)

Command Purpose

To specify the metrics to be assigned to redistributed routers for Routing Information Protocol next generation (RIPng), use the default-metric command in router configuration mode.

To return to the default state, use the no form of this command.

Command Syntax

default-metric *NUMBER-VALUE*

no default-metric

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	Metric value	1-16

Command Mode

Router Configuration

Default

By default, the metric is set to 1.

Usage

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with

incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Examples

The following example shows a switch using both the RIPv6 and the Open Shortest Path First (OSPFv3) routing protocols. The example advertises OSPFv3-derived routes using RIPv6 and assigns the OSPFv3-derived routes a RIPv6 metric of 10:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)#default-metric 10
Switch(config-router)#redistribute ospfv3
```

Related Commands

redistribute (RIPv6)

7.2.7 distance (RIPv6)

Command Purpose

To define an administrative distance for routes that are inserted into the routing table, use the distance command in router configuration mode.

To return the administrative distance to its default distance definition, use the no form of this command.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual switch or a group of switches. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value is, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

Command Syntax

distance *DISTANCE*
no distance

Parameter	Parameter Description	Parameter Value
DISTANCE	Administrative distance	1-255.(routes with a distance value of 255 are not installed in the routing table)

Command Mode

Router Configuration

Default

By default, the distance is 120.

Usage

Route Source	Default Distance
Connected interface	0
Static route	1
External Border Gateway Protocol (eBGP)	20
Open Shortest Path First (OSPF)	110
Routing Information Protocol (RIP)/ Routing Information Protocol next generation (RIPv6)	120
Internal BGP	200
Unknown	255
Unknown	255

Examples

The following example set the distance of RIPv6 投 200:


```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#distance 200
```

Related Commands

None

7.2.8 neighbor (RIPng)

Command Purpose

To specify a neighboring router to which to notify routing updating information, use the neighbor command in router configuration mode.

To remove the neighbor, use the no form of this command.

Command Syntax

```
neighbor IPV6_ADDR IFNAME
no neighbor IP-ADDRESS IFNAME
```

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	Link-local IP address of a peer switch with which routing information will be notified	IPv6 Address
IFNAME	Interface name to which the neighbor is specified	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

No neighboring switches are defined.

Usage

Especially use the neighbor command in conjunction with the passive-interface command to send routing updates to specific neighbors. This command permits the point-to-point (non-multicast) notification of routing update information. Multiple neighbors can be configured

Examples

In the following example, RIPng updates are sent to all interfaces which have been enabled RIPng routing except eth-0-1. However, in this case a neighbor switch configuration command is included. This command permits the sending of routing updates to specific neighbors:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# passive-interface eth-0-1
Switch(config-router)# neighbor fe80:db8::1 eth-0-1
```

Related Commands

router rip

7.2.9 offset-list (RIPng)

Command Purpose

To add an offset to incoming and outgoing metrics to routes exchanging via Routing Information Protocol next generation (RIPng), use the offset-list command in router configuration mode.

To remove an offset list, use the no form of this command.

Command Syntax

offset-list *ACCESSS-LIST-NAME* (in | out) *METRIC-OFFSET* (*IFNAME* |)
 no offset-list (in | out) (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
ACCESSS-LIST-NAME	Named access list to be applied	Up to 40 characters
in	Applies the access list to incoming metrics	-
out	Applies the access list to outgoing metrics	-
METRIC- OFFSET	Positive offset to be applied to metrics for networks matching the access list. The meric-offset range is 0 to 16	0-16
IFNAME	Interface name to which the offset list is applied	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

This command is configured by default.

Usage

Especially if the offset value is added to the routing metric by offset-list, the default action where the metric updates when RIPng message arrives (as RFC defined) is ignored, but outputs will be added.

The offset value is added to the routing metric. An offset list with an interface is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

Examples

In the following example, the switch applies an offset of 10 if access list 21 permits:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# offset-list 21 out 10
```

Related Commands

None

7.2.10 passive-interface (RIPng)

Command Purpose

To disable sending routing updates for the Routing Information Protocol next generation (RIPng) on an interface, use the passive-interface command in router configuration mode.

To enable the sending of routing updates, use the no form of this command.

Command Syntax

```
passive-interface IFNAME
no passive-interface IFNAME
```

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

Interface is active by default.

Usage

The command disable the sending of routing updates and ignore the request message from neighbor on an interface, but updates from other routers on that interface should be received and processed.

Examples

The following example sets the interface eth-0-1 as passive:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# passive-interface eth-0-1
```

Related Commands

router ipv6 rip

7.2.11 redistribute (RIPng)

Command Purpose

To redistribute routes from one routing domain into RIPng routing domain, use the redistribute command in router configuration mode. To disable redistribution, use the no form of this command.

Command Syntax

```
redistribute PROTOCOL { [ metric VALUE ] | route-map NAME }
no redistribute PROTOCOL
```

Parameter	Parameter Description	Parameter Value
PROTOCOL	The name of a routing protocol, or the keyword connected, or static. If you specify a routing protocol, use one of the following keywords: bgp, and ospfv3, static, connected,isis	connected/static/bgp/ospf/isis
metric VALUE	(Optional) When redistributing other routing process to the RIP process, the default metric is 1 if no metric value is specified	1-16
route-map NAME	Route map reference, name of route-map entry	Up to 20 characters

Command Mode

Router Configuration

Default

Route redistribution is disabled.
Metric-value: 1

Usage

The metric value specified in the redistribute command supersedes the metric value specified using the default-metric command.

Examples

The following example redistributes the static routes into RIPng with metric 10:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#redistribute static metric 10
```

Related Commands

default-metric

7.2.12 timers basic (RIPng)

Command Purpose

To adjust Routing Information Protocol next generation (RIPng) network timers, use the timers basic command in router configuration mode.

To restore the default timers, use the no form of this command.

Command Syntax

```
timers basic UPDATE TIMEOUT INVALID
no timers basic
```

Parameter	Parameter Description	Parameter Value
UPDATE	Rate (in seconds) at which updates are sent. This is the fundamental timing parameter of the routing protocol	5-2147483647 seconds
TIMEOUT	Time (in seconds) after which a route is declared invalid without updates that refresh the route. The route then enters into an invalid state and is not used for forwarding packets. It is marked inaccessible and advertised as unreachable	5-2147483647 seconds
INVALID	Time after which an invalid route is removed from RIPng routing database	5-2147483647 seconds

Command Mode

Router Configuration

Default

Update timer: 30 seconds
Timeout timer: 180 seconds
Invalid timer: 120 seconds

Usage

The basic timing parameters for RIPv6 are adjustable. Because RIPv6 is executing a distributed, asynchronous routing algorithm, these timers must be the same for all switches and access servers in the network.

Examples

The following example sets updates to every 5 seconds. If a switch is not learned from in 15 seconds, the route is declared unusable. And after 15 seconds the invalid route will be removed from RIPv6 routing database:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)#timers basic 5 15 15
```

Related Commands

None

7.2.13 distribute-list(RIPv6)

Command Purpose

To filter networks in routing updates, use the distribute-list command in router configuration mode.
To restore the default value, use the no form of this command.

Command Syntax

```
distribute-list ( prefix NAME | ACCESS-LIST-NAME ) ( in | out ) ( IFNAME | )
no distribute-list ( prefix name | ACCESS-LIST-NAME ) ( in | out ) ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
prefix NAME	Filter prefixes in routing update	Up to 40 characters
ACCESS-<i>LIST-NAME</i>	Access-list name	Up to 40 characters
in	Filter incoming routing updates	-
out	Filter outgoing routing updates	-
IFNAME	The interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following example filters the received RIPv6 routes:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# distribute-list prefix 1 in
```

Related Commands

ipv6 prefix-list

7.2.14 aggregate-address (RIPng)

Command Purpose

To specify an aggregate RIPng route announcement, use the aggregate-address command in router configuration mode. To disable this feature, use the no form of this command.

Command Syntax

```
aggregate-address IPV6_PREFIX ( avoid-feedback | ) IFNAME
no aggregate-address IP-ADDRESS IFNAME
```

Parameter	Parameter Description	Parameter Value
IPV6_PREFIX	Specify an aggregate network (IPv6 address prefix and length).	IPv6 Address and mask length in X::X::X/M format
avoid-feedback	Forbid to learn the address which is the same to aggregate address from the interface	-
IFNAME	The interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

No aggregate address is defined.

Usage

If the routing info is suppressed by aggregate-address, it is still stored in RIPng database, but won't be notified to neighbor. On the other hand the aggregate-address will be notified to neighbor. The command only be useful when the interface is L3.

Examples

In the following example, RIPng specify an aggregate address into RIPng database:

```
Switch# configure terminal
Switch(config)#router ipv6 rip
Switch(config-router)# aggregate-address 2001:db8::/32
```

Related Commands

None

7.2.15 route map(RIPng)

Command Purpose

Use this command to set a route map for input or output filtering on a specified interface. Use the no parameter with this command to disable this function.

Command Syntax

```
route-map NAME ( in | out ) IFNAME
no route-map name ( in | out ) IFNAME
```

Parameter	Parameter Description	Parameter Value
NAME	route map name	Up to 20 characters
in	route map for input filtering	-
out	route map for output filtering	-

Parameter	Parameter Description	Parameter Value
IFNAME	Specify an interface name to which to associate the route map	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

None.

Usage

None

Examples

In the following example, set a route map for input filtering interface eth-0-1:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# route-map routemap10 in eth-0-1
```

Related Commands

None

7.2.16 maximum-prefix(RIPng)

Command Purpose

Use this command to configure the maximum prefix. Use the no parameter with this command to disable the limiting of the number of RIPng routes in the routing table.

Command Syntax

maximum-prefix *NUMBER-VALUE* (*PERCENTAGE-VALUE* |)
no maximum-prefix

Parameter	Parameter Description	Parameter Value
NUMBER-VALUE	maximum number of RIPng routes allowed	1-65535
PERCENTAGE-VALUE	Percentage of maximum routes to generate a warning.The default threshold is 75%.	1-100

Command Mode

Router Configuration

Default

None.

Usage

Use this command to configure the maximum prefix.

Examples

In the following example, set maximum RIPng prefix is 700 and warning percentage is 70%:

```
Switch# configure terminal
Switch(config)# router ipv6 rip
Switch(config-router)# maximum-prefix 700 70
```

Related Commands

None

7.2.17 show ipv6 rip database

Command Purpose

Use this command to display RIPv6 information database.

Command Syntax

show ipv6 rip database

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip database command:

Switch# show ipv6 rip database

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

Network	Next Hop	If	Met Tag	Time
Rc 2001:db8:0:6::/64	::	eth-0-9	1	0
Rc 2001:db8:0:49::/64	::	eth-0-48	1	0

Related Commands

show ipv6 rip interface

7.2.18 show ipv6 rip interface

Command Purpose

To display summary information of Routing Information Protocol next generation (RIPv6) for a specific interface, use the show ip rip interface command in privileged EXEC mode.

Command Syntax

show ipv6 rip interface (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip interface command:

```
Switch# show ipv6 rip interface eth-0-9
```

```
eth-0-9 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
  IPv6 interface address:
    2001:db8:0:6::2/64
    fe80::b4df:82ff:fe70:ec00/10
```

Related Commands

show ipv6 rip database

7.2.19 show ipv6 rip database database-summary

Command Purpose

Use this command to display the summary statistics for RIPng database.

Command Syntax

show ipv6 rip database database-summary

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ip rip database database-summary command:

```
Switch# show ipv6 rip database database-summary
```

Type	Count
RIPng connected	2
Total	2

Related Commands

show ipv6 rip database

7.2.20 show ipv6 protocol rip

Command Purpose

To show Routing Information Protocol next generation (RIPng), use the show ipv6 protocol rip command in privileged EXEC mode.

Command Syntax

show ipv6 protocol rip

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show ipv6 rip interface command:

```
Switch# show ipv6 protocol rip
```

```
Routing Protocol is "ripng"  
  Sending updates every 30 seconds with +/-50%, next due in 2949331570 seconds  
  Timeout after 180 seconds, garbage collect after 120 seconds  
  Outgoing update filter list for all interface is not set  
  Incoming update filter list for all interface is not set  
  Default redistribute metric is 1  
  Redistributing:  
    Interface  
      eth-0-9  
      eth-0-48  
  Routing for Networks:  
  Number of routes (including connected): 2  
  Distance: (default is 120)
```

Related Commands

None

7.2.21 debug ipv6 rip

Command Purpose

Use this command to specify the options for the displayed debugging information for RIPng events, RIPng packets.
Use the no parameter with this command to disable all debugging.

Command Syntax

```
debug ipv6 rip ( all | events | packet | )  
no debug ripv6 ( all | events | packet | )  
no debug all ipv6 ( rip | )
```

Parameter	Parameter Description	Parameter Value
all	All RIPng debug information	-
events	RIPng events debug information is displayed	-
packet	packet (recv send) (detail) Specifies RIPng packets only	-
recv		-
send		-
detail		-

Command Mode

Privileged EXEC

Default

Disabled

Usage

None

Examples

The following example displays information about the ripng packets that are received and sent out from the connected router:
Switch# debug ipv6 rip packet

Related Commands

show debugging rip

7.2.22 show debugging ipv6 rip

Command Purpose

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging.

Command Syntax

show debugging ipv6 rip

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the debug status of RIPng.

Examples

The following is sample output from the show debugging ripng command:
Switch# show debugging ipv6 rip

RIPng debugging status:
RIPng event debugging is on

Related Commands

debug ipv6 rip

7.2.23 show resource ipv6 rip

Command Purpose

Use this command to display the route resources used by RIPng protocol.

Command Syntax

show resource ipv6 rip

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource ipv6 rip command:

```
Switch# show resource ipv6 rip
```

RIPng Resource	Used	Capability
Routes	2	728

Related Commands

```
show ipv6 rip database
```

7.2.24 clear ipv6 rip route

Command Purpose

To clear the specifical route in RIPng routing table, use the command clear ipv6 rip router in privileged exec mode.

Command Syntax

```
clear ipv6 rip route ( IPV6_PREFIX | connected | static | ospfv3 | bgp | all )
```

Parameter	Parameter Description	Parameter Value
IPV6_PREFIX	Removes entries which exactly match this destination address from the RIPng routing table	IPv6 Address and mask length in X:X::X/M format
connected	Removes entries for connected routes from the RIPng routing table	-
static	Removes static entries from the RIPng routing table	-
ospfv3	Removes only OSPF routes from the RIPng routing table	-
bgp	Removes only BGP routes from the RIPng routing table	-
all	Removes the entire RIPng routing table	-

Command Mode

Privileged EXEC

Default

None.

Usage

Use this command to clear specific data from the RIPng routing table.

Examples

In the following example, clear the entire RIPng routing table:

```
Switch# clear ipv6 rip route all
```

Related Commands

None

7.3 IPv6UC Commands

7.3.1 ipv6 enable

Command Purpose

Use this command to enable ipv6 function. Use the no form of this command to disable ipv6 function.

Command Syntax

```
ipv6 enable
no ipv6 enable
```

Command Mode

Global Configuration

Default

Ipv6 function is disabled by default.

Usage

This command is used to enable the ipv6 function globally. Ipv6 packet should be processed as a L2 packet when ipv6 function is disabled.

Examples

The following example shows how to enable IPv6:

```
Switch# configure terminal
Switch(config)# ipv6 enable
```

Related Commands

None

7.3.2 max-static-v6routes

Command Purpose

To configure the maximum ipv6 static routes in system, use the max-static-v6routes command in global configuration mode. To configure the maximum static routes to default value, use the no form of this command.

Command Syntax

```
max-static-v6routes COUNT
no max-static-v6routes
```

Parameter	Parameter Description	Parameter Value
COUNT	The count of maximum ipv6 static routes.	1-65535

Command Mode

Global Configuration

Default

Please reference the current TCAM profile.

Usage

Users should not configure the maximum ipv6 static routes more than system profile of FIB. Also, users should not configure the maximum ipv6 static routes less than the current static routes count.

Examples

The following example displays how to change maximum ipv6 static routes to 10:

```
Switch# configure terminal
Switch(config)# max-static-v6routes 10
```

Related Commands

```
show ipv6 route
```

7.3.3 ipv6 route

Command Purpose

To establish ipv6 static routes, use the ipv6 route command in global configuration mode.
To remove ipv6 static routes, use the no form of this command.

Command Syntax

```
ipv6 route vrf NAME DEST_PREFIX ( GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFNULL ) ( ADMIN_DISTANCE | )
ipv6 route DEST_PREFIX ( GLOBAL_PREFIX | LINK_LOCAL IFNAME | IFTUNNEL | IFNULL ) ( ADMIN_DISTANCE | )
no ipv6 route vrf NAME DEST_PREFIX ( GLOBAL_PREFIX | LINK_LOCAL ( IFNAME | ) | IFNULL | )
no ipv6 route DEST_PREFIX ( GLOBAL_PREFIX | LINK_LOCAL ( IFNAME | ) | IFTUNNEL | IFNULL | )
```

Parameter	Parameter Description	Parameter Value
vrf NAME	VRF instance name	Up to 15 characters
DEST_PREFIX	IPv6 route prefix (in format X:X::X:X/M) for the destination	IPv6 Address and mask length in X:X::X:X/M format
GLOBAL_PREFIX	IPv6 route global unicast address (in format X:X::X:X) for the nexthop	IPv6 Address in X:X::X:X format
LINK_LOCAL	IPv6 route link local address (FE80::/10) for the nexthop	IPv6 Address in X:X::X:X format
IFNAME	Outgoing interface for the ipv6 route	Support physical/aggregation/vlan/tunnel ports
IFTUNNEL	Tunnel interface name for the ipv6 route	tunnel <0-1023>
IFNULL	null 0 interface for the ipv6 route	null 0
ADMIN_DISTANCE	(Optional) An administrative distance. The default administrative distance for a static route is 1. This configuration is optional.	1-255

Command Mode

Global Configuration

Default

There is not any static IPv6 route configured by default.

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ipv6 route 3001::1/64 fe80::1234 eth-0-2
Switch(config)# ipv6 route vrf a 3002::1/64 3001::1
```

Related Commands

```
show ipv6 route
```

7.3.4 ipv6 address

Command Purpose

To set an IPv6 address for an interface, use the `ipv6 address` command in interface configuration mode. To remove an IPv6 address, use the `no` form of this command.

Command Syntax

```
ipv6 address GOLBAL_PREFIX ( eui-64 | )
no ipv6 address GOLBAL_PREFIX ( eui-64 | )
ipv6 address LINK-LOCAL link-local
no ipv6 address LINK-LOCAL link-local
ipv6 address auto link-local
no ipv6 address auto link-local
no ipv6 address
```

Parameter	Parameter Description	Parameter Value
GOLBAL_PREFIX	Global IPv6 address and prefix length. In X:X::X/M format	IPv6 Address and mask length in X:X::X/M format
LINK-LOCAL	Link-local IPv6 address. In X:X::X:X format	IPv6 Address in X:X::X:X format

Command Mode

Interface Configuration

Default

There is not any ipv6 address on the interface by default.

Usage

Use this command to configure ipv6 address on the interface. Use the `no` form of this command to remove the ipv6 address. This configuration should not affect the ipv4 functions and other ipv6 configuration on the interface.

The maximum count of the Link-local address is 1; the maximum count of the global address address is 8.

Use this command with the keyword "auto link-local" to automatically generate a link-local address, if there is no link-local address on this interface. Use the `no` form of this command with the keyword "auto link-local" to remove the automatically generated link-local address, if there is only that automatically generated link-local address left on this interface.

Use this command with a specified ipv6 address (e.g. 3ffe:506::1/48) to configure a global unicast ipv6 address. Use this command with the keyword "eui-64" to generate interface id automatically by the eui-64 algorithm. The global address should not be same. Use the `no` form of this command to remove the specified ipv6 global unicast address.

If there is no link-local address on the interface, system should automatically generate one when configure a global unicast ipv6 address.

Use this command with a specified ipv6 address (e.g. fe80::1) and a keyword "link-local" to configure a link-local address. Use the `no` form of this command with the specified ipv6 address and the keyword "link-local" to remove the specified ipv6 link-local address. The specified link-local address has a higher priority than the automatically generated the link-local address, that can overwrite the automatically generated one.

Use the `no` form of this command without any parameters or keywords to remove all ipv6 addresses on the interface, include ipv6 global addresses and link-local addresses.

Examples

The following example shows how to configure link local address and global unicast address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 address fe80::1233 link-local
Switch(config-if)# ipv6 address 3001:1::1234/64
```

Related Commands

```
show ipv6 interface
```

7.3.5 show ipv6 route

Command Purpose

Use this command to show the ipv6 routes.

Command Syntax

```
show ipv6 route ( vrf NAME | ) ( database | )
show ipv6 route ( vrf NAME | ) ( database | ) ( bgp | connected | ospf | rip | static )
show ipv6 route ( vrf NAME | ) IPV6_ADDRESS
show ipv6 route ( vrf NAME | ) IPV6_PREFIX
show ipv6 route ( vrf NAME | )
show ipv6 route ( vrf NAME | ) summary
```

Parameter	Parameter Description	Parameter Value
IPV6_PREFIX	IPv6 prefix in X:X::X:X/M format	IPv6 Address and mask length in X:X::X:X/M format

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to show the ipv6 routes

Examples

The following example shows the result of this command:

```
Switch# show ipv6 route
```

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
Timers: Uptime
S      3001::/64 [1/0]
      via fe80::1234, eth-0-2, 04:09:56
C      3001:1::/64
      via ::, eth-0-1, 01:39:07
C      3001:1::1234/128
      via ::1, eth-0-1, 01:39:07
S      3002::/64 [1/0]
      via 3001::1 (recursive via fe80::1234), eth-0-2, 04:09:19
C      3ffe:2::/64
      via ::, eth-0-2, 1d19h37m
C      3ffe:2::10/128
      via ::1, eth-0-2, 1d19h37m
C      fe80::/10
      via ::, Null0, 1d19h53m
```

```
Switch# show ipv6 route database
```

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
      > - selected route, * - FIB route, p - stale info
Timers: Uptime
S      > 3001::/64 [1/0]
      * via fe80::1234, eth-0-2, 04:10:45
C      > 3001:1::/64
      * via ::, eth-0-1, 01:39:56
C      > 3001:1::1234/128
      * via ::1, eth-0-1, 01:39:56
S      > 3002::/64 [1/0]
```



```

    * via 3001::1 (recursive via fe80::1234), eth-0-2, 04:10:08
C    > 3ffe:2::/64
    * via ::, eth-0-2, 1d19h37m
C    > 3ffe:2::10/128
    * via ::1, eth-0-2, 1d19h37m
C    > fe80::/10
    * via ::, Null0, 1d19h54m

Switch# show ipv6 route static

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
      [*] - [AD/Metric]
Timers: Uptime
S      3001::/64 [1/0]
      via fe80::1234, eth-0-2, 04:11:42
S      3002::/64 [1/0]
      via 3001::1 (recursive via fe80::1234), eth-0-2, 04:11:05

Switch# show ipv6 route 3001::64

Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:12:32 ago
  * via fe80::1234, eth-0-2

Switch# show ipv6 route 3001::64/64

Routing entry for 3001::/64
  Known via "static", distance 1, metric 0, best
  Last update 04:13:03 ago
  * via fe80::1234, eth-0-2

Switch# show ipv6 route summary

IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 8
Route source networks
connected          5
static             2
Total              7

```

Related Commands

ipv6 route

7.3.6 show ipv6 interface

Command Purpose

Use this command to show the ipv6 ipv6 statues on the interface.

Command Syntax

show ipv6 interface (*IFNAME* |) (brief |)

Parameter	Parameter Description	Parameter Value
IFNAME	IPv6 interface status and configuration	Support physical/aggregation/loopback/vlan/tunnel ports
brief	Brief summary of IPv6 status and configuration	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows the result of this command:

```
Switch# show ipv6 interface eth-0-1
```

```
Interface eth-0-1
  Interface current state: UP
  The maximum transmit unit is 1500 bytes
  IPv6 is enabled, link-local address is fe80::1233
  Global unicast address(es):
    3001:1::1234, subnet is 3001:1::/64
  Joined group address(es):
    ff02::1:ff00:1234
    ff02::1:ff00:0
    ff02::1:ff00:1233
    ff02::2
    ff02::1
  ICMP error messages limited to one every 2000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  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 max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
Switch # show ipv6 interface eth-0-1 brief
*down: administratively down
Interface      Status  Protocol  IPv6 address
eth-0-1        up      up         3001:1::1234
               fe80::1233
```

```
Switch# show ipv6 interface eth-0-1 brief
```

```
*down: administratively down
Interface      Status  Protocol  IPv6 address
eth-0-1        up      up         3001:1::1234
               fe80::1233
```

Related Commands

ipv6 enable
ipv6 address

7.3.7 ipv6 verify unicast reverse-path

Command Purpose

Use this command to enable urpf (unicast reverse path forwarding) on the interface. Use the no form of this command to disable urpf on the interface.

Command Syntax

ipv6 verify unicast reverse-path
no ipv6 verify unicast reverse-path

Command Mode

Interface Configuration

Default

Urp is disabling on the interface by default.

Usage

Use this command to enable urpf (unicast reverse path forwarding) on the interface. Use the no form of this command to disable urpf on the interface.

Examples

The following example shows how to enable URPF for IPv6:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 verify unicast reverse-path
```

Related Commands

show ipv6 interface

7.3.8 ipv6 icmp error-interval

Command Purpose

Use this command to set the ipv6 icmp error-interval. Use the no form of this command to set the ipv6 icmp error-interval to default.

Command Syntax

```
no ipv6 icmp error-interval ERROR_INTERVAL
no ipv6 icmp error-interval
```

Parameter	Parameter Description	Parameter Value
error-interval	ICMPv6 Error message interval.	0–2147483647 ms

Command Mode

Global Configuration

Default

1000 milliseconds.

Usage

None

Examples

The following example shows how to set the ICMPv6 error interval:

```
Switch# configure terminal
Switch(config)# ipv6 icmp error-interval 2000
```

Related Commands

None

7.3.9 clear ipv6 route static

Command Purpose

Use this command to clear static ipv6 routes.

Command Syntax

```
clear ipv6 route static
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to clear ipv6 static routes:

```
Switch# clear ipv6 route static
```

Related Commands

None

7.4 Ipv6 Prefix-list Commands

7.4.1 ipv6 prefix-list

Command Purpose

To create a ipv6 prefix list or add a prefix-list entry, use the ipv6 prefix-list command in global configuration mode. To delete a prefix-list or an entry, use the no form of this command.

Command Syntax

```
ipv6 prefix-list WORD [ seq SEQUENCE-NUMBER ] ( deny | permit ) ( any | IPv6-ADDRESS/M [ ge GE-LENGTH ] [ le LE-LENGTH ] )
no ipv6 prefix-list WORD [ seq SEQUENCE-NUMBER ] ( deny | permit ) ( any | IPv6-ADDRESS/M [ ge GE-LENGTH ] [ le LE-LENGTH ] )
no ipv6 prefix-list WORD [ seq SEQUENCE-NUMBER ]
```

Parameter	Parameter Description	Parameter Value
WORD	Config a name to identify the prefix list	Up to 40 characters
seq SEQUENCE-NUMBER	Applies a sequence number to a prefix-list entry. The range of sequence number that can be entered is from 1 to 65535. If a sequence number is not entered when configuring this command, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5	1-65535
deny	Denies access for a matching condition	-
permit	Permits access for a matching condition	-

Parameter	Parameter Description	Parameter Value
IPv6-ADDRESS /M	Configures the network address, and the length of the network mask in bits. The network number can be any valid IPv6 address or prefix. The bit mask can be a number from 0 to 128	IPv6 address and mask length between 1-128
ge GE-LENGTH	(Optional)Specifies the lesser value of a range (the "from" portion of the range description) by applying the ge-length argument to the range specified. The ge-length argument represents the minimum prefix length to be matched	1-128
le LE-LENGTH	(Optional)Specifies the greater value of a range (the "to" portion of the range description) by applying the le-length argument to the range specified. The le-length argument represents the maximum prefix length to be matched	1-128

Command Mode

Global Configuration

Default

No prefix lists are created.

Usage

The `ipv6 prefix-list` command is used to configure IPv6 prefix filtering. Prefix lists are configured with `permit` or `deny` keywords to either permit or deny the prefix based on the matching condition. A prefix list consists of an IPv6 address and a bit mask. The IPv6 address can be global address, or a link-local address. The bit mask is entered as a number from 1 to 128. An implicit deny is applied to traffic that does not match any prefix-list entry. Prefix lists are configured to match an exact prefix length or a prefix range. The `ge` and `le` keywords are used to specify a range of the prefix lengths to match, providing more flexible configuration than can be configured with just the `network/length` argument. The prefix list is processed using an exact match when neither the `ge` nor `le` keyword is entered. If only the `ge` value is entered, the range is the value entered for the `ge ge-length` argument to a full 128-bit length. If only the `le` value is entered, the range is from value entered for the `network/length` argument to the `le le-length` argument. If both the `ge ge-length` and `le le-length` keywords and arguments are entered, the range falls between the values used for the `ge-length` and `le-length` arguments. The following formula shows this behavior:

`network/length < ge ge-length < le le-length <= 128`.

A prefix list is configured with a name and/or sequence number. One or the other must be entered when configuring this command. If a sequence number is not entered, a default sequence number of 5 is applied to the prefix list. And subsequent prefix list entries will be incremented by 5 (for example, 5, 10, 15, and onwards). If a sequence number is entered for the first prefix list entry but not subsequent entries, then the subsequent entries will also be incremented by 5 (For example, if the first configured sequence number is 3, then subsequent entries will be 8, 13, 18, and onwards). Default sequence numbers can be suppressed by entering the `no` form of this command with the `seq` keyword. Prefix lists are evaluated starting with the lowest sequence number and continues down the list until a match is made. Once a match is made that covers the network the `permit` or `deny` statement is applied to that network and the rest of the list is not evaluated.

Examples

The following example shows how to configure `ipv6 prefix-list`: To deny the default route `::/0`:

```
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc deny ::/0
To permit the prefix 2001:db8::/64:
```

```
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc permit 2001:db8::/64
To accept a mask length of up to 64 bits in routes with the prefix 2001:db8::/32:
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc permit 2001:db8::/32 le 64
To deny mask lengths greater than 64 bits in routes with the prefix 2001:db8::/32:
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc deny 2001:db8::/32 ge 64
```

Related Commands

ipv6 prefix-list description
ipv6 prefix-list sequence
show ipv6 prefix-list
clear ipv6 prefix-list

7.4.2 ipv6 prefix-list description

Command Purpose

To add a text description of a ipv6 prefix list, use the ipv6 prefix-list description command in global configuration mode. To remove the text description, use the no form of this command

Command Syntax

```
ipv6 prefix-list WORD description LINE
no ipv6 prefix-list WORD description [ LINE ]
```

Parameter	Parameter Description	Parameter Value
WORD	Name of prefix list	Up to 40 characters
LINE	The description of this prefix-list	Up to 80 characters

Command Mode

Global Configuration

Default

There is no description for prefix-list.

Usage

The ipv6 prefix list will be created if it didn't exist.

Examples

The following example shows how to add description:

```
Switch# configure terminal
Switch(config)# ipv6 prefix-list abc description Permit routes from customer A
```

Related Commands

ipv6 prefix-list
ipv6 prefix-list sequence
show ipv6 prefix-list
clear ipv6 prefix-list

7.4.3 ipv6 prefix-list sequence-number

Command Purpose

To enable the generation of sequence numbers for entries in a ipv6 prefix list, use the ipv6 prefix-list sequence-number command in global configuration mode. To disable this function, use the no form of this command.

Command Syntax

```
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number
```

Command Mode

Global Configuration

Default

This command has no default behavior.

Usage

This command is used to enable sequence-number display.

Examples

The following example shows how to enable ipv6 prefix-list sequence-number:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 prefix-list sequence-number
```

Related Commands

```
ipv6 prefix-list
show ipv6 prefix-list
clear ipv6 prefix-list
```

7.4.4 show ipv6 prefix-list

Command Purpose

To show ipv6 prefix list information, use the show ipv6 prefix-list command.

Command Syntax

```
show ipv6 prefix-list ( summary | detail | ) ( WORD | )
show ipv6 prefix-list WORD ( seq SEQUENCE-NUMBER | IPv6-ADDRESS /M ( longer | first-match | ) )
```

Parameter	Parameter Description	Parameter Value
summary	Summary of prefix lists	-
detail	Detail of prefix lists	-
WORD	Name of the prefix list	Up to 40 characters
seq SEQUENCE-NUMBER	sequence number of the entry in the ipv6 prefix list	1-65535
IPv6-ADDRESS /M	IPv6 prefix <network>/<length>, e.g., 2001:db8::/32	IPv6 address and mask length between 1-128
longer	Lookup longer prefix	-
first-match	First matched prefix	-

Command Mode

Privileged EXEC

Default

This command has no default behavior.

Usage

None

Examples

The following example shows how to display ip prefix-list:

```
Switch# show ipv6 prefix-list
```

```

ipv6 prefix-list ripng_pre: 5 entries
seq 1 deny 2001:db8:9::/64
seq 2 deny 2001:db8:10::/64
seq 3 deny 2001:db8:11::/64
seq 4 deny 2001:db8:12::/64
seq 5 permit any

```

Related Commands

```

ipv6 prefix-list
clear ipv6 prefix-list

```

7.4.5 clear ipv6 prefix-list

Command Purpose

To Resets the hit count of the prefix list entries, use the clear ipv6 prefix-list command.

Command Syntax

```
clear ipv6 prefix-list ( WORD ( IPv6-ADDRESS /M | ) | )
```

Parameter	Parameter Description	Parameter Value
WORD	Name of the prefix list	Up to 40 characters
IPv6-ADDRESS /M	IPv6 prefix <network>/<length>, e.g., 2001:db8::/32	IPv6 address and mask length between 1-128

Command Mode

Privileged EXEC

Default

This command has no default behavior.

Usage

None

Examples

The following example shows how to clear ipv6 prefix-list:

```
Switch(config)# clear ipv6 prefix-list test
```

Related Commands

```
ipv6 prefix-list
```

7.5 Route Map Commands

7.5.1 route-map

Command Purpose

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing in bgp, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

Command Syntax

```

route-map MAP-TAG [ permit | deny ] [ sequence-NUMBER ]
no route-map MAP-TAG [ permit | deny ] [ SEQUENCE_NUMBER ]

```


Parameter	Parameter Description	Parameter Value
MAP-TAG	A meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.	The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.
	permit	-
	deny	-
SEQUENCE_NUMBER	(Optional) Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted	1-65535

Command Mode

Global Configuration

Default

The permit keyword is the default.

Usage

None

Examples

The following example shows how to create a route-map and enter route-map configuration mode:

```
Switch# configure terminal
Switch(config)# route-map rip-to-ospf permit
Switch(config-route-map)# match metric 1
Switch(config-route-map)# set metric 2
```

Related Commands

match as-path
 match community
 match interface
 match ip address
 match local-preference
 match metric
 match origin
 match route-type
 match tag
 set aggregator
 set as-path
 set atomic-aggregate
 set comm-list
 set community
 set dampening
 set extcommunity
 set ip address
 set local-preference
 set metric
 set metric-type
 set origin
 set originator-id
 set tag
 set vpv4
 set weight

7.5.2 match as-path

Command Purpose

Use this command to match an autonomous system path access list.

Use the no parameter with this command to remove a path list entry.

The match as-path command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met then the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match as-path *LISTNAME*
 no match as-path

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies as autonomous system path access list name	Up to 20 characters

Command Mode

Route-map Configuration

Default

No match as-path is specified by default.

Usage

This command is valid only for BGP.

Examples

```

Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match as-path myaccesslist
  
```

Related Commands

match metric
match ip address
match community
set as-path
set community

7.5.3 match community

Command Purpose

Use this command to specify the community to be matched.

Use the no parameter with this command to remove the community list entry.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

Use the match community command to allow matching based on community lists.

The values set by the match community command overrides the global values. The route that does not match at least one match clause is ignored.

Command Syntax

match community *WORD*
no match community

Parameter	Parameter Description	Parameter Value
WORD	Specifies the Community-list name	Up to 40 characters

Command Mode

Route-map Configuration

Default

No match community is specified by default.

Usage

This command is valid only for BGP.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match community mylist
```

Related Commands

match ip address
match as-path
set as-path
set community
match metric

7.5.4 match interface

Command Purpose

Use this command to define the interface match criterion.

Use the no parameter with this command to remove the specified match criterion..

The match interface command specifies the next-hop interface name of a route to be matched.

Command Syntax

match interface *IFNAME*
no match interface

Parameter	Parameter Description	Parameter Value
IFNAME	A string that specifies the interface for matching	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Route-map Configuration

Default

No match interface is specified by default.

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match interface eth-0/1
```

Related Commands

match tag
match route-type external

7.5.5 match ipv6 address

Command Purpose

Use this command to specify the match address of route.

Use the no parameter with this command to remove the match ipv6 address entry.

The match ipv6 address command specifies the IPv6 address to be matched. If there is a match for the specified IPv6 address, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

```
match ipv6 address ACCESSLISTID
no match ipv6 address
```

Parameter	Parameter Description	Parameter Value
ACCESSLISTID	Specify a IPv6 access-list name, up to 20 characters	Up to 20 characters

Command Mode

Route-map Configuration

Default

No match ipv6 address is specified by default.

Usage

This command is valid for BGP, OSPFv3 and RIPng only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# match ipv6 address List1
```

Related Commands

```
match community
match as-path
set as-path
set community
match metric
```

7.5.6 match ipv6 address prefix-list

Command Purpose

Use this command to match entries of ipv6 prefix-lists.

Use the no parameter with this command to disable this function.

This command specifies the entries of prefix-lists to be matched. If there is a match for the specified ipv6 prefix-list entries, and permit is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

```
match ipv6 address prefix-list LISTNAME
no match ipv6 address prefix-list (LISTNAME | )
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the IPv6 prefix list name	Up to 40 characters

Command Mode

Route-map Configuration

Default

No match ipv6 address prefix-list is specified by default.

Usage

This command is valid for BGP, OSPFv3 and RIPv6 only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ipv6 address prefix-list mylist
```

Related Commands

```
match community
match as-path
set as-path
set community
match metric
```

7.5.7 match ipv6 next-hop

Command Purpose

Use this command to specify a ipv6 next-hop address to be matched in a route-map.

Use the no parameter with this command to disable this function.

The match ipv6 next-hop command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is

specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match ipv6 next-hop (*IPv6_ADDR* | *ACCESSLISTID*)

no match ipv6 next-hop [*IPv6-ADDRESS* | *ACCESSLISTID*]

Parameter	Parameter Description	Parameter Value
IPv6_ADDR	Specify a IPv6 address, e.g., 2001:db8::1	IPv6 Address
ACCESSLISTID	Specify a IPv6 access-list name	up to 20 characters

Command Mode

Route-map Configuration

Default

No match ipv6 next-hop is specified by default.

Usage

This command is valid for BGP, OSPFv3 and RIPv6 only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# match ipv6 next-hop mylist
```

Related Commands

match community
match as-path
set as-path
set community
match metric

7.5.8 match ipv6 next-hop prefix-list

Command Purpose

Use this command to specify the next-hop IPv6 address match criterion, using the prefix-list.

Use the no parameter with this command to remove the specified match criterion.

Use the match ipv6 next-hop prefix-list command to match the next-hop IPv6 address of a route.

Command Syntax

match ipv6 next-hop prefix-list *LISTNAME*

no match ipv6 next-hop prefix-list [*LISTNAME*]

Parameter	Parameter Description	Parameter Value
LISTNAME	A string specifying the ipv6 prefix-list name	-

Command Mode

Route-map Configuration

Default

No match ipv6 next-hop prefix-list is specified by default.

Usage

This command is valid for RIPvng only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match ipv6 next-hop prefix-list list1
```

Related Commands

match metric
match interface
match ip next-hop

7.5.9 match local-preference

Command Purpose

Use this command to specify the local-preference match criterion.
Use the no parameter with this command to remove the specified match criterion.
Use the match local-preference command to match the local preference of a route.

Command Syntax

match local-preference *LOCAL-PREFERENCE*
no match local-preference

Parameter	Parameter Description	Parameter Value
LOCAL-PREFERENCE	Species the preference value	0-4294967295

Command Mode

Route-map Configuration

Default

No match local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# match local-preference 100
```

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

7.5.10 match metric

Command Purpose

Use this command to match a metric of a route.
Use the no parameter with this command to disable this function.
The match metric command specifies the metric to be matched. If there is a match for the specified metric, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match metric *METRICVAL*
no match metric

Parameter	Parameter Description	Parameter Value
METRICVAL	metric value	0-4294967295

Command Mode

Route-map Configuration

Default

No match metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# no match metric
```

Related Commands

match community
match as-path
set as-path
set community
match ip next-hop

7.5.11 match origin

Command Purpose

Use this command to match origin code.

Use the no parameter with this command to disable this matching.

The origin attribute defines the origin of the path information. The *egp* parameter is indicated as an *e* in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The *igp* parameter is indicated as an *i* in the routing table, and it indicates the origin of the path information is interior to the originating AS.

The *incomplete* parameter is indicated as a *?* in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The match origin command specifies the origin to be matched. If there is a match for the specified origin, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Command Syntax

match origin { *egp* | *igp* | *incomplete* }
no match origin

Parameter	Parameter Description	Parameter Value
egp	learned from EGP	-
igp	Local IGP	-
incomplete	Unknown heritage	-

Command Mode

Route-map Configuration

Default

No match origin is specified by default.

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute deny 34
Switch(config-route-map)# match origin egp
```

Related Commands

None

7.5.12 match route-type

Command Purpose

Use this command to match specified external route type.

Use the no parameter with this command to turn off the matching.

Use the match route-type external command to match specific external route types. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes, and external type-2 matches only Type 2 external routes.

Command Syntax

```
match route-type external { type-1 | type-2 }
no match route-type external
```

Parameter	Parameter Description	Parameter Value
type-1	Match OSPF External Type 1 metrics	-
type-2	Match OSPF External Type 1 metrics	-

Command Mode

Route-map Configuration

Default

No match route-type is specified by default.

Usage

This command is valid for OSPF only

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match route-type external type-1
```

Related Commands

match tag

7.5.13 match tag

Command Purpose

Use this command to match the specified tag value.
 Use the no parameter with this command to turn off the declaration.
 Use the match tag command to match the specified tag value.

Command Syntax

match tag *TAG*
 no match tag

Parameter	Parameter Description	Parameter Value
TAG	Specifies the tag value	0-4294967295

Command Mode

Route-map Configuration

Default

No match tag is specified by default.

Usage

This command is valid for OSPF RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 10
Switch(config-route-map)# match tag 100
```

Related Commands

match metric
 match route-type external

7.5.14 set ipv6 aggregator

Command Purpose

Use this command to set the AS number for the route map and router ID.
 Use the no parameter with this command to disable this function.
 An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the set aggregator command to assign an AS number for the aggregator.
 To use the set aggregator command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
 If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set ipv6 aggregator as *ASNUM IPV6_ADDR*
 no set ipv6 aggregator

Parameter	Parameter Description	Parameter Value
ASNUM	Specifies the AS number of aggregator	1-65535
IPV6_ADDR	Specifies the IPv6 address of aggregator	IPv6 Address

Command Mode

Route-map Configuration

Default

No set aggregator is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set aggregator as 43 2001:db8::1
```

Related Commands

None

7.5.15 set as-path

Command Purpose

Use this command to modify an autonomous system path for a route.

Use the no parameter with this command to disable this function.

Use the set as-path command to specify an autonomous system path. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use the prepend parameter with this command to prepend an AS path string to routes increasing the AS path length.

To use the set as-path command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set as-path prepend ASN [...ASN]

no set as-path

Parameter	Parameter Description	Parameter Value
ASN	System prepends this number to the AS path	1-4294967295
prepend	Prepends the autonomous system path	-

Command Mode

Route-map Configuration

Default

No set as-path is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map myroute permit 3
Switch(config-route-map)# set as-path prepend 8 24
```

Related Commands

None

7.5.16 set atomic-aggregate

Command Purpose

Use this command to set an atomic aggregate attribute.

Use the no parameter with this command to disable this function

To use the set atomic aggregate command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set atomic-aggregate
no set atomic-aggregate
```

Command Mode

Route-map Configuration

Default

No set atomic-aggregate is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set atomic-aggregate
```

Related Commands

None

7.5.17 set comm-list delete

Command Purpose

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the no parameter with this command to disable this feature.

Command Syntax

```
set comm-list { STANDARD | EXPANDED | WORD } delete
no set comm-list
```

Parameter	Parameter Description	Parameter Value
STANDARD	Standard community-list number	1-99
EXPANDED	Expanded community-list number	100-199
WORD	Name of the Community-list	up to 255 characters
delete	Delete matching communities	-

Command Mode

Route-map Configuration

Default

No set comm-list is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set comm-list 34 delete
```

Related Commands

None

7.5.18 set community

Command Purpose

Use this command to set the communities attribute.

Use the no parameter with this command to delete the entry.

Use this command to set the community attribute and group destinations in a certain community, as well as, apply routing decisions according to those communities.

To use the set community command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set community [ AA:NN | internet | local-AS | no-advertise | no-export ]
```

```
set community none
```

```
no set community
```

Parameter	Parameter Description	Parameter Value
AA:NN	AA:NN: Specifies the community number in this format AA = The AS number NN = The number assigned to community	Support 2 bytes AS number and 4 bytes community ID
internet	Specifies the Internet (well-known community)	-
local-AS	Specifies no sending outside the local AS (well-known community)	-
no-advertise	Specifies no advertisement of this route to any peer (well-known community)	-
no-export	Specifies no advertisement of this route to next AS (well-known community)	-
none	Removes the community attribute from the prefixes that pass the route-map	-

Command Mode

Route-map Configuration

Default

No set community is specified by default.

Usage

This command is valid for BGP only.

Examples

The following examples show the use of the set community command with different parameters:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-export no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community no-advertise
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set community 10:01 23:34 12:14 no-export
```

Related Commands

None

7.5.19 set dampening

Command Purpose

Use this command to enable route-flap dampening and set parameters.

Use the no parameter with this command to disable it.

Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Command Syntax

set dampening *REACHTIME REUSE SUPPRESS MAXSUPPRESS* [*UNREACHTIME*]

no set dampening

Parameter	Parameter Description	Parameter Value
REACHTIME	Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes	1-45
REUSE	Specifies the reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750	1-20000
SUPPRESS	Specifies the suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000	1-20000
MAXSUPPRESS	Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes)	1-255

Parameter	Parameter Description	Parameter Value
UNREACHTIME	Specifies the un-reachability half-life time for penalty, in minutes. The default value is 15 minutes	1-45

Command Mode

Route-map Configuration

Default

Reference to the syntax description above.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map R1 permit 24
Switch(config-route-map)# set dampening 20 333 534 30
```

Related Commands

None

7.5.20 set extcommunity**Command Purpose**

Use this command to set an extended community attribute.

Use the no parameter with this command to disable this function

To use the set extcommunity command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set extcommunity { rt | soo } EXTCOMMNUMBER [ ...EXTCOMMNUMBER ]
no set extcommunity { rt | soo }
```

Parameter	Parameter Description	Parameter Value
rt	Specifies the route target of the extended community	-
soo	Specifies the site-of-origin of the extended community	-
EXTCOMMNUMBER	ASN:NN_or_IP-address:nn VPN extended community	-
ASN:NN	the AS number	Support 2 bytes AS number and 4 bytes community ID
IPADDRESS	the AS number in IP address form	IPv4 Address

Command Mode

Route-map Configuration

Default

No set extcommunity is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 06:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity rt 0.0.0.6:01
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 06:01
Switch# configure terminal
Switch(config-route-map)# route-map rmap1 permit 3
Switch(config-route-map)# set extcommunity soo 0.0.0.6:01
```

Related Commands

None

7.5.21 set ipv6 next-hop

Command Purpose

Use this command to set the specified next-hop ipv6 address value.

Use the no parameter with this command to turn off the setting.

Use this command to set the next-hop IPv6 address to the routes.

Command Syntax

```
set ipv6 next-hop [ local ] IPV6_ADDR
```

```
no set ipv6 next-hop [ local ]
```

Parameter	Parameter Description	Parameter Value
local	Link-local address	-
IPV6_ADDR	Specifies the IPv6 address of the next-hop	IPv6 Address

Command Mode

Route-map Configuration

Default

No set ipv6 next-hop is specified by default.

Usage

This command is valid for BGP, OSPFv3, and RIPng only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set ipv6 next-hop 2001:db8::1
```

Related Commands

None

7.5.22 set local-preference

Command Purpose

Use this command to set the specified local-preference value.
Use the no parameter with this command to turn off the setting.
Use this command to set the local-preference value of the routes

Command Syntax

set local-preference *LOCAL-PREFERENCE*
no set local-preference

Parameter	Parameter Description	Parameter Value
LOCAL-PREFERENCE	Species the preference value	0-4294967295

Command Mode

Route-map Configuration

Default

No set local-preference is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map mymap permit 3
Switch(config-route-map)# set local-preference 100
```

Related Commands

None

7.5.23 set metric

Command Purpose

Use this command to set a metric value for a route.
Use the no parameter with this command to disable this function.
This command sets the metric value for a route, and influences external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the bgp always-compare-med command.
To use the set metric command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.
If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set metric *METRICVAL*
no set metric

Parameter	Parameter Description	Parameter Value
METRICVAL	metric value	0-4294967295

Command Mode

Route-map Configuration

Default

No set metric is specified by default.

Usage

This command is valid for BGP, OSPF and RIP.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric 600
```

Related Commands

None

7.5.24 set metric-type

Command Purpose

Use this command to set the metric type for the destination routing protocol.

Use the no parameter with this command to return to the default.

This command sets the type to either Type-1 or Type-2 in the AS-external-LSA when the route-map matches the condition.

Command Syntax

```
set metric-type { TYPE1 | TYPE2 }
no set metric-type
```

Parameter	Parameter Description	Parameter Value
type1	Select to set external type 1 metric	-
type2	Select to set external type 2 metric	-

Command Mode

Route-map Configuration

Default

No set metric-type is specified by default.

Usage

This command is valid for OSPF only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set metric-type 1
```

Related Commands

None

7.5.25 set origin

Command Purpose

Use this command to set the BGP origin code.

Use the no parameter with this command to delete an entry.

The origin attribute defines the origin of the path information. The three parameters with this command indicate three different values. IGP is interior to the originating AS. This happens if IGP is redistributed into the BGP. EGP is learned through an Exterior Gateway Protocol. Incomplete is unknown or learned through some other means. This happens when static route is redistributed in BGP and the origin of the route is incomplete.

To use the set origin command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set origin { egp | igp | incomplete }
no set origin

Parameter	Parameter Description	Parameter Value
egp	Specifies a remote EGP system	-
igp	A local IGP system	-
incomplete	Specifies a system of unknown heritage	-

Command Mode

Route-map Configuration

Default

No set origin is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set origin egp
```

Related Commands

None

7.5.26 set ipv6 originator-id

Command Purpose

Use this command to set the originator ID attribute.

Use the no parameter with this command to disable this function

To use the set originator-id command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set ipv6 originator-id *IPv6_ADDR*
no set ipv6 originator-id

Parameter	Parameter Description	Parameter Value
IPv6_ADDR	Specifies the IPv6 address of originator	IPv6 Address

Command Mode

Route-map Configuration

Default

No set originator-id is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set ipv6 originator-id 2001:db8::1
```

Related Commands

None

7.5.27 set tag

Command Purpose

Use this command to set a specified tag value.

Use the no parameter with this command to return to the default.

Tag in this command is the route tag which is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. Also, with using route-map, ZebOS can tag the LSAs with the appropriate tag value. Sometimes, the tag matches with using route-map, and sometimes, the value may be used by another application.

Command Syntax

```
set tag TAGVALUE
no set tag
```

Parameter	Parameter Description	Parameter Value
TAGVALUE	Tag value for destination routing protocol.	0-4294967295

Command Mode

Route-map Configuration

Default

No set tag is specified by default.

Usage

This command is valid for OSPF and RIP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set tag 6
```

Related Commands

```
redistribute
default-information
```

7.5.28 set vpnv6 next-hop

Command Purpose

Use this command to set a VPNv6 next-hop address.

Use the no parameter with this command to disable this function

To use the set vpnv6-next-hop command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

```
set vpnv6 next-hop IPV6_ADDR
```

no set vpnv6 next-hop

Parameter	Parameter Description	Parameter Value
IPv6_ADDR	Specifies the IPv6 address of originator	IPv6 Address

Command Mode

Route-map Configuration

Default

No set vpnv6 next-hop is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set vpnv6 next-hop 2001:db8::1
```

Related Commands

None

7.5.29 set weight

Command Purpose

Use this command to set weights for the routing table.

Use the no parameter with this command to delete an entry.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

To use the set weight command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met

match as-path 10

set weight 400

In the above configuration, all routes that apply to access-list 10 will have the weight set at 400.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Command Syntax

set weight *WEIGHT*

no set weight

Parameter	Parameter Description	Parameter Value
WEIGHT	Specifies the weight value	0-4294967295

Command Mode

Route-map Configuration

Default

No set weight is specified by default.

Usage

This command is valid for BGP only.

Examples

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 3
Switch(config-route-map)# set weight 60
```

Related Commands

match as-path

7.5.30 show route-map

Command Purpose

Use this command to display user readable route-map information.

Command Syntax

show route-map [*NAME*]

Parameter	Parameter Description	Parameter Value
NAME	route-map name	The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch1# show route-map
route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
```

Related Commands

route-map

7.6 IPv6 BGP Commands

7.6.1 address-family

Command Purpose

Use this command to enter the IPv6 address-family command mode.

Command Syntax

address-family ipv6 (unicast |)

Parameter	Parameter Description	Parameter Value
unicast	Specifies unicast prefixes.	-

Command Mode

Router Configuration

Default

None

Usage

Use the address family command to enter the address family mode allowing configuration of address-family specific parameters. To leave the address family mode and return to the Configure mode use the exit-address-family command.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router)address-family ipv6
```

Related Commands

exit-address-family

7.6.2 aggregate-address**Command Purpose**

Use this command to configure BGP aggregate entries.
Use the no parameter with this command to disable this function.

Command Syntax(no) aggregate-address *IPADDRESS* { summary-only | as-set }

Parameter	Parameter Description	Parameter Value
IPv6_ADDR	X::X::X/M Specifies the aggregate prefix	IPv6 address
summary-only	Filters more specific routes from updates.	-
as-set	Generates AS set path information	-

Command Mode

Address Family Configuration

Default

Disabled

Usage

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. The aggregate-address command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the summary-only parameter advertises the prefix only, suppressing the more-specific routes to all neighbors.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# aggregate-address 2018::1/64 as-set summary-only
```

Related Commands

N/A

7.6.3 bgp always-compare-med

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the no parameter with this command to disallow the comparison.

Command Syntax

(no) bgp always-compare-med

Command Mode

Router Configuration

Default

Disabled

Usage

Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

MED comparison is done only among paths from the same autonomous system (AS). Use bgp always-compare-med command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp always-compare-med
```

Related Commands

bgp bestpath med
bgp bestpath as-path ignore

7.6.4 bgp bestpath as-path ignore

Command Purpose

Use this command to prevent the router from considering as-path as a factor in the algorithm for choosing a route. Use the no parameter with this command to allow the router to consider as-path in choosing a route.

Command Syntax

(no) bgp bestpath as-path ignore

Command Mode

Router Configuration

Default

Disabled

Usage

None

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath as-path ignore
```


Related Commands

bgp always-compare-med, bgp bestpath med, bgp bestpath compare-routerid

7.6.5 bgp bestpath compare-confed-aspath

Command Purpose

Use this command to allow comparing of the confederation AS path length.

Use the no parameter with this command to revert the selection and ignore AS confederation path length in the BGP best path selection.

Command Syntax

(no) bgp bestpath compare-confed-aspath

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been specified.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-confed-aspath
```

Related Commands

bgp bestpath as-path ignore

7.6.6 bgp bestpath compare-routerid

Command Purpose

Use this command to compare router-id for identical eBGP paths.

Use the no parameter with this command to disable this function.

Command Syntax

(no) bgp bestpath compare-routerid

Command Mode

Router Configuration

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Usage

When comparing similar routes from peers the BGP router does not consider router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with lowest router ID is selected. The router-id is the highest IP address on the router, with preference given to loopback addresses. Router-id can be manually set by using the bgp router-id command.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath compare-routerid
```

Related Commands

```
show bgp ipv6
show ip bgp neighbors
```

7.6.7 bgp bestpath med

Command Purpose

Use this command to specify Multi Exit Discriminator (MED) attribute comparison.
Use the no parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax

```
bgp bestpath med confed [ missing-as-worst ]
bgp bestpath med missing-as-worst [ confed ]
no bgp bestpath med confed [ missing-as-worst ]
no bgp bestpath med missing-as-worst [ confed ]
```

Parameter	Parameter Description	Parameter Value
confed	Compares MED among confederation paths	-
missing-as-worst	Treats missing MED as the least preferred one	-

Command Mode

Router Configuration

Default

MED value is zero.

Usage

Use this command to specify two MED attributes—confed and missing-as-worst. The confed attribute enables MED comparison among paths learned from confederation peers. The MEDs are compared only if there is no external autonomous system (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made.
The missing-as-worst attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If missing-as-worst is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp bestpath med missing-as-worst
```

Related Commands

bgp-always-compare-med, bgp bestpath as-path ignore, bgp deterministic-med

7.6.8 bgp client-to-client reflection

Command Purpose

Use this command to restore route reflection from a BGP route reflector to clients.
Use the no parameter with this command to turn off client-to-client reflection.

Command Syntax

```
bgp client-to-client reflection
no bgp client-to-client reflection
```

Parameter	Parameter Description	Parameter Value
reflection	Allows reflection of routes	-

Command Mode

Router Configuration

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Usage

The bgp client-to-client reflection command is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use no bgp client-to-client reflection command to disable the client-to-client route reflection.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) no bgp client-to-client reflection
```

Related Commands

```
bgp cluster-id
neighbor route-reflector-client
show bgp ipv6
```

7.6.9 bgp cluster-id

Command Purpose

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. Use the no parameter with this command to remove the cluster ID.

Command Syntax

```
bgp cluster-id CLUSTERID
no bgp cluster-id
```

Parameter	Parameter Description	Parameter Value
CLUSTERID	A.B.C.D <1-4294967295> Specifies the cluster ID of this router acting as a route reflector, either as IP address or as a maximum of 4 bytes.	IPv4 Address or Number between 1-4294967295
A.B.C.D	A.B.C.D Route Reflector Cluster-id in IP address format	IPv4 Address
<1-4294967295>	Route Reflector cluster-id as a 32 bit quantity	1-4294967295

Command Mode

Router Configuration

Default

N/A

Usage

A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The `bgp cluster-id` command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp cluster-id 1.1.1.1
```

Related Commands

`bgp client-to-client reflection`, `neighbor route-reflector-client`, `show bgp ipv6`

7.6.10 bgp confederation identifier

Command Purpose

Use this command to specify a Bgp confederation identifier.

Use the `no` parameter with this command to remove the Bgp confederation identifier.

Command Syntax

```
bgp confederation identifier ID
no bgp confederation identifier
```

Parameter	Parameter Description	Parameter Value
ID	Set routing domain confederation AS number	1-65535

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation identifier 1
```

Related Commands

`bgp confederation peer`

7.6.11 bgp confederation peers

Command Purpose

Use this command to configure the Autonomous Systems (AS) that belong to the confederation.

Use the `no` parameter with this command to remove an autonomous system from the confederation.

Command Syntax

```
bgp confederation peers .ASN
no bgp confederation peers ( .ASN | )
```

Parameter	Parameter Description	Parameter Value
ASN	AS numbers of eBGP peers that are under same confederation but in a different sub-AS	1-65535

Command Mode

Router Configuration

Default

N/A

Usage

A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation. Use the `bgp confederation peer` command to define the list of confederation peers.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp confederation peers 1234 21345
```

Related Commands

`bgp confederation identifier`

7.6.12 bgp dampening

Command Purpose

Use this command to set bgp dampening parameters.
Use the `no` parameter with this command to unset the bgp dampening parameters.

Command Syntax

```
bgp dampening REACHTIME
bgp dampening REACHTIME REUSE
bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS ( UNREACHTIME | )
bgp dampening route-map ROUTEMAP
no bgp dampening REACHTIME
no bgp dampening REACHTIME REUSE
no bgp dampening REACHTIME REUSE SUPPRESS MAXSUPPRESS ( UNREACHTIME | )
no bgp dampening route-map ROUTEMAP
```

Parameter	Parameter Description	Parameter Value
REUSE	Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750 SUPPRESS <1-20000> Specifies the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000.	1-20000

Parameter	Parameter Description	Parameter Value
SUPPRESS	Specifies suppress-time. A route dampening more than this value will be suppressed. The default value is 2000.	1-20000
MAXSUPPRESS	Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes).	1-255
REACHTIME	Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes.	1-45
UNREACHTIME	Specifies the un-reachability half-life time for penalty, in minutes.	1-45
ROUTEMAP	route-map WORD Route-map to specify criteria for dampening.	The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is un-suppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 800 2500 80 25
```

Related Commands

N/A

7.6.13 bgp default local-preference

Command Purpose

Use this command to change the default local preference value.
Use the no parameter with this command to revert to the default setting.

Command Syntax

bgp default local-preference *PREF_VALUE*
no default local-preference (*PREF_VALUE* |)

Parameter	Parameter Description	Parameter Value
	Configure default local preference	
PREF_VALUE	value. The default local preference value is 100.	0-4294967295

Command Mode

Router Configuration

Default

The default local preference value is 100.

Usage

Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. Use bgp default local-preference command to define preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp default local-preference 2345555
```

Related Commands

N/A

7.6.14 bgp deterministic-med

Command Purpose

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system.

Use the no parameter with this command to disallow this setting.

Command Syntax

bgp deterministic-med
no bgp deterministic-med

Command Mode

Router Configuration

Default

Disabled

Usage

"Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. Enable bgp deterministic med command on all routers in the local AS, for a correct comparison result. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value.

Based on this comparison, the best path is then chosen.

This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp always-compare-med command."

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp deterministic-med
```

Related Commands

show bgp ipv6, show bgp ipv6 neighbors

7.6.15 bgp enforce-first-as

Command Purpose

Use this command to specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied.
Use the no parameter with this command to disable this feature.

Command Syntax

```
bgp enforce-first-as
no bgp enforce-first-as
```

Command Mode

Router Configuration

Default

Disabled

Usage

Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp enforce-first-as
```

Related Commands

N/A

7.6.16 bgp fast-external-failover

Command Purpose

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down.
Use the no parameter with this command to disable this feature.

Command Syntax

```
bgp fast-external-failover
no bgp fast-external-failover
```

Command Mode

Router Configuration

Default

Enabled

Usage

None

Examples


```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp fast-external-failover
```

Related Commands

N/A

7.6.17 bgp log-neighbor-changes

Command Purpose

Use this command to enable logging of status change messages without turning on debug bgp commands. Use the no parameter with this command to disable this feature.

Command Syntax

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

Command Mode

Router Configuration

Default

Disabled

Usage

System implementation provides other kinds of logging services for neighbor status, for example, debug bgp fsm, debug bgp events, etc. However, these commands create a significant hit in the logging performance. The bgp log-neighbor-changes command, logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Examples

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp log-neighbor-changes
```

Related Commands

N/A

7.6.18 bgp router-id

Command Purpose

Use this command to configure the router identifier.

Use the no parameter with this command to disable this function

Command Syntax

bgp router-id *ROUTERID*
no bgp router-id (*ROUTERID* |)

Parameter	Parameter Description	Parameter Value
ROUTERID	A.B.C.D Manually configured router ID.	In IPv4 Address format

Command Mode

Router Configuration
Address Family Configuration

Default

In case the loopback interface is configured the router-id is set to the IP address of a loopback interface. If not, the highest IP address is the router-id.

Usage

Use bgp router-id command to manually configure a fixed router ID as a BGP router identifier.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp router-id 1.1.2.3
```

Related Commands

N/A

7.6.19 bgp scan-time

Command Purpose

Use this command to set the interval for BGP route next-hop scanning.
Use the no parameter with this command to disable this function.

Command Syntax

bgp scan-time *TIME*
no bgp scan-time (*TIME* |)

Parameter	Parameter Description	Parameter Value
TIME	Scanning interval in seconds. The default scanning interval is 60 seconds.	0-60

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database.
To disable BGP scanning, set the scan time interval to 0 seconds.

Examples

```
Switch# configure terminal
Switch(config) router bgp 100
Switch(config-router) bgp scan-time 10
```

Related Commands

N/A

7.6.20 clear bgp ipv6 *

Command Purpose

Use this command to reset a BGP connection for all peers.

Command Syntax

```
clear bgp ipv6 * ( in | out | soft | )
clear bgp ipv6 * vrf NAME
```

Parameter	Parameter Description	Parameter Value
*	clears all bgp peers	-
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
soft	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
vrf	VPN routing/forwarding instance	-
NAME	VPN Routing/Forwarding instance name	Up to 16 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

There are two kinds BGP reset, hard reset will clear BGP peers and establish again. Soft reset only refresh routing table.

Examples

```
Switch# clear bgp ipv6 *
Switch# clear bgp ipv6 * soft
Switch# clear bgp ipv6 * vrf aa
```

Related Commands

N/A

7.6.21 clear bgp ipv6 X:X::X:X

Command Purpose

Use this command to reset a IPv6 BGP connection for a specific IPv6 address.

Command Syntax

```
clear bgp ipv6 X:X::X:X ( in | out | soft )
clear ipv6 bgp X:X::X:X vrf NAME
```

Parameter	Parameter Description	Parameter Value
X:X::X:X	Specifies the IPv6 address of the BGP route to be cleared	IPv6 address
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
soft	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-
vrf	VPN routing/forwarding instance	-
NAME	VPN Routing/Forwarding instance name	Up to 16 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear bgp ipv6 2018::1
Switch# clear bgp ipv6 2018::1 soft
```

Related Commands

N/A

7.6.22 clear bgp ipv6 unicast dampening

Command Purpose

Use this command to reset all dampened BGP routes under the specified address family.

Command Syntax

```
clear bgp ipv6 dampening ( X:X::X:X | X:X::X:X/M | )
```

Parameter	Parameter Description	Parameter Value
X:X::X:X	Specifies the IPv6 address for which Bgp dampening is to be cleared.	IPv6 address
X:X::X:X/M	Specifies the IPv6 address with mask for which Bgp dampening is to be cleared.	IPv6 address with mask length

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear bgp ipv6 unicast dampening
Switch# clear bgp ipv6 unicast dampening 2018::1
```

Related Commands

N/A

7.6.23 clear bgp ipv6 unicast flap-statistics

Command Purpose

Use this command to clear the flap count and history duration for all the prefixes under the specified address family.

Command Syntax

clear bgp ipv6 unicast flap-statistics (*X::X::X* | *X::X::X/M* |)

Parameter	Parameter Description	Parameter Value
<i>X::X::X</i>	Specifies the IPv6 address for which Bgp dampening is to be cleared.	IPv6 address
<i>X::X::X/M</i>	Specifies the IPv6 address with mask for which Bgp dampening is to be cleared.	IPv6 address with mask length

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear bgp ipv6 unicast flap-statistics 10.10.0.121
```

Related Commands

N/A

7.6.24 clear bgp ipv6 ASN

Command Purpose

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax

clear bgp ipv6 *ASN* (in | out | soft |)

Parameter	Parameter Description	Parameter Value
ASN	Specifies the AS Number for which all routes will be cleared	1-4294967295
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
soft	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# clear bgp ipv6 100

Related Commands

N/A

7.6.25 clear bgp ipv6 external**Command Purpose**

Use this command to reset a BGP connection for all external peers.

Command Syntax

clear bgp ipv6 external (in | soft |)

Parameter	Parameter Description	Parameter Value
external	Clears all external peers	-
in	Indicates that incoming advertised routes will be cleared	-
soft	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# clear bgp ipv6 external in
```

Related Commands

N/A

7.6.26 clear bgp ipv6 peer-group**Command Purpose**

Use this command to reset a BGP connection for all members of a peer group.

Command Syntax

```
clear bgp ipv6 peer-group WORD ( in | out | soft | )
```

Parameter	Parameter Description	Parameter Value
peer-group	Clears all members of a peer group	-
WORD	Specifies the name of the peer group for which all members will be cleared.	Up to 20 characters
in	Indicates that incoming advertised routes will be cleared	-
out	Indicates that outgoing advertised routes will be cleared.	-
soft	soft (in out) Indicates that both incoming and outgoing routes will be cleared	-

Command Mode

Privileged EXEC

Default

N/A

Usage

None

Examples

```
Switch# clear bgp ipv6 peer-group Peer1 out
```

Related Commands

N/A

7.6.27 debug bgp**Command Purpose**

Use this command to specify all debugging options for BGP. Use the no parameter with this command to disable this function.

Command Syntax

```
debug bgp ( all | dampening | events | filters | fsm | keepalives | mpls | updates )
```

no debug bgp (all | dampening | events | filters | fsm | keepalives | mpls | nsm | updates)

Parameter	Parameter Description	Parameter Value
all	Used with the no form exclusively; turns off all debugging for BGP	-
dampening	Specifies debugging for Bgp dampening.	-
events	Specifies debugging for BGP events.	-
filters	Specifies debugging for BGP filters.	-
fsm	Specifies debugging for BGP Finite State Machine (FSM).	-
mpls	Specifies debuggin for BGP Multiprotocol Label Switching.	-
keepalives	Specifies debugging for BGP keepalives.	-
updates	updates Specifies debugging for BGP updates.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

This command without any parameters turns on normal bgp debug information.

Examples

```
Switch# debug bgp
Switch# debug bgp events
```

Related Commands

N/A

7.6.28 exit-address-family

Command Purpose

Use this command to exit the address family mode.

Command Syntax

exit-address-family

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example shows the use of exit-address-family command and the change in the prompt after using this command:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# address-family ipv6
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

Related Commands

address-family

7.6.29 neighbor activate

Command Purpose

Use this command to enable the exchange of the specified AF routes with a neighboring router.
Use the no parameter with this command to disable exchange of information with a neighbor.

Command Syntax

```
neighbor NEIGHBORID activate
no neighbor NEIGHBORID activate
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	-

Command Mode

Router Configuration

Address Family Configuration

Default

N/A

Usage

After the TCP connection is opened with the neighbor, this command is used to enable or disable the exchange of the specified AF information with a neighboring router.

To enable the exchange of multicast and VPNv4 address prefix types, neighbors are activated using the neighbor activate command in address family mode.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 active
```

Related Commands

neighbor remote-as

7.6.30 neighbor advertisement-interval

Command Purpose

Use this command to set the minimum interval between sending the BGP routing updates.
Use the no parameter with this command to set the interval time to default.

Command Syntax

neighbor *NEIGHBORID* advertisement-interval *TIME*
no neighbor *NEIGHBORID* advertisement-interval *TIME*

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	-
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	-
TIME	Advertise -interval value in seconds	0-600

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to set the minimum interval between the sending of BGP routing updates. To reduce the flapping of routes to internet, a minimum advertisement interval is set, so that the BGP routing updates are sent only per interval seconds. bgp dampening can also be used to control the effects of flapping routes.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 advertisement-interval 45
```

Related Commands

N/A

7.6.31 neighbor allowas-in

Command Purpose

Use this command to configure PE routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs).
Use the no parameter with this command to disable the readvertisement of a PE router's ASN.

Command Syntax

neighbor *NEIGHBOR* allowas-in [*NUMBER*]
no neighbor *NEIGHBOR* allowas-in

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
NUMBER	Number of occurrences of AS number. Default value is 1	1-10

Command Mode

Address Family Configuration

Default

Disabled

Usage

In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Use the neighbor allowas-in command to configure two VRFs on each PE router to receive and re-advertise prefixes. One of the VRFs receives prefixes with ASNs from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with ASNs from the CE router and re-advertises them to all PE routers in the hub and spoke configuration.

Control the number of times an ASN is advertised, by specifying a number from 1 to 10.

Examples

```
Switch# configure terminal
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 allowas-in 3
```

Related Commands

N/A

7.6.32 neighbor attribute-unchanged

Command Purpose

Use this command to advertise unchanged BGP attributes to the specified neighbor.
Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* attribute-unchanged { as-path | next-hop | med }
no neighbor *NEIGHBORID* attribute-unchanged { as-path | next-hop | med }

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group.	Up to 20 characters
	For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	
as-path	AS path attribute	-
next-hop	Next hop attribute	-
med	Multi Exit Discriminator	-

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 23018::1 attribute-unchanged as-path med
```

Related Commands

N/A

7.6.33 neighbor capability orf prefix-list**Command Purpose**

Use this command to advertise ORF capability to neighbors.
 Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor NEIGHBORID capability orf prefix-list ( both | receive | send )
no neighbor NEIGHBORID capability orf prefix-list ( both | receive | send )
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group.	Up to 20 characters
	For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	
orf	Advertises ORF capability to its neighbors	-
both	Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.	-
receive	Indicates that the local router is willing to receive ORF entries from its peer	-
send	Indicates that the local router is willing to send ORF entries to its peer	-

Command Mode

Address Family Configuration

Default

N/A

Usage

Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates. The local router advertises the ORF capability in send mode and the remote router receives the ORF capability in receive mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 1.1.1.1 capability orf prefix-list both
```

Related Commands

N/A

7.6.34 neighbor default-originate

Command Purpose

Use this command to allow a BGP local router to send the default route 0:0::0:0 to a neighbor for use as a default route. Use the no parameter with this command to send no route as a default.

Command Syntax

```
neighbor NEIGHBORID default-originate ( ROUTEMAP | )
no neighbor NEIGHBORID default-originate ( ROUTEMAP | )
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
ROUTEMAP	route-map WORD	-
route-map	The route-map to specify criteria to originate default routes	-
WORD	Route-map name	-

Command Mode

Address Family Configuration

Default

N/A

Usage

Every router should have a default route, it is used to send datas to the network which is not existent in local RIB. To set a default route on each router can make every router have a default route, or to create a default route and broadcast it to BGP peer by this command.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 default-originate route-map myroute
```

Related Commands

N/A

7.6.35 neighbor description

Command Purpose

Use this command to associate a description with a neighbor.
Use the no parameter with this command to remove the description.

Command Syntax

```
neighbor NEIGHBORID description LINE
no neighbor NEIGHBORID description
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
LINE	Text to describing the neighbor.	Up to 80 characters

Command Mode

Router Configuration

Default

N/A

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 description Backup router for sales.
```

Related Commands

N/A

7.6.36 neighbor distribute-list**Command Purpose**

Use this command to filter route update from a particular BGP neighbor.
Use the no parameter with this command to remove an entry.

Command Syntax

```
neighbor NEIGHBORID distribute-list WORD ( in | out )
no neighbor NEIGHBORID distribute-list WORD ( in | out )
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Parameter	Parameter Description	Parameter Value
WORD	The name of IP access-list	Up to 20 characters
in	Indicates that incoming advertised routes will be filtered.	-
out	Indicates that outgoing advertised routes will be filtered.	-

Command Mode

Address Family Configuration

Default

N/A

Usage

Use only one distribute-list per BGP neighbor.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 distribute-list mylist out
```

Related Commands

N/A

7.6.37 neighbor ebgp-multihop

Command Purpose

Use this command to accept and attempt BGP connections to external peers on indirectly connected networks. Use the no parameter with this command to return to the default.

Command Syntax

```
neighbor NEIGHBORID ebgp-multihop ( COUNT | )
no neighbor NEIGHBORID ebgp-multihop
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
COUNT	Maximum hop count. If the maximum hop count is not set the hop count is 255.	1-255

Command Mode

Router Configuration

Default

N/A

Usage

Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 remote-as 20
Switch(config-router)# neighbor 2018::1 ebgp-multihop 5
```

Related Commands

N/A

7.6.38 neighbor filter-list

Command Purpose

Use this command to set up a BGP filter.

Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* filter-list *LISTNAME* (in | out)
no neighbor *NEIGHBORID* filter-list *LISTNAME* (in | out)

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
in	Indicates that incoming advertised routes will be filtered.	-
out	Indicates that outgoing advertised routes will be filtered.	-
LISTNAME	The name of an autonomous system path access list.	Up to 20 characters

Command Mode

Address Family Configuration

Default

N/A

Usage

This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 filter-list listname out
```

Related Commands

N/A

7.6.39 neighbor maximum-prefix**Command Purpose**

Use this command to control the number of prefixes that can be received from a neighbor.
Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor NEIGHBORID maximum-prefix MAXIMUM
no neighbor NEIGHBORID maximum-prefix
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
MAXIMUM	MAXPREFIX (THRESHOLD) (warning-only)	-
MAXPREFIX	Specifies the maximum number of prefixes permitted.	1-4294967295
THRESHOLD	<1-100> Specifies the threshold value, 1 to 100 percent.	1-100
warning-only	Only gives a warning message when the limit is exceeded.	-

Command Mode

Address Family Configuration

Default

N/A

Usage

The neighbor maximum-prefix command allows the configuration of a specified number of prefixes that a BGP router is allowed to receive from a neighbor. When the warning-only option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the clear ip bgp command is used.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 maximum-prefix 1244 warning-only
```

Related Commands

N/A

7.6.40 neighbor next-hop-self

Command Purpose

Use this command to configure the router as the next hop for a BGP-speaking neighbor or peer group. Use the no parameter with this command to disable this feature.

Command Syntax

```
neighbor NEIGHBORID next-hop-self
no neighbor NEIGHBORID next-hop-self
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Address Family Configuration

Default

N/A

Usage

This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 10.10.0.72 next-hop-self
```

Related Commands

N/A

7.6.41 neighbor override-capability

Command Purpose

Use this command to override a capability negotiation result.
Use the no parameter with this command to disable this function

Command Syntax

neighbor *NEIGHBORID* override-capability
no neighbor *NEIGHBORID* override-capability

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 2018::1 override-capability
```

Related Commands

N/A

7.6.42 neighbor passive

Command Purpose

Use this command to set a BGP neighbor as passive.
Use the no parameter with this command to disable this function

Command Syntax

(no) neighbor *NEIGHBORID* passive

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# neighbor 2018::1 passive
```

Related Commands

N/A

7.6.43 neighbor peer-group (adding a neighbor)

Command Purpose

Use this command to add a neighbor to an existing peer-group.
Use the no parameter with this command to disable this function.

Command Syntax

```
neighbor IPADDRESS peer-group TAG
no neighbor IPADDRESS peer-group
```

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	X:X::X:X Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
	X:X::X:X Specifies the address of the BGP neighbor in IPv6 format.	
	TAG Name of the peer-group	

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group.	Up to 20 characters
	For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	

Command Mode

Router Configuration

Default

N/A

Usage

Use this command to Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the neighbor peer-group create command and then use this command to add neighbors to the group.

Examples

This example shows a new peer-group group1 and the adding of a neighbor 2018::1 to the group:

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
Switch(config-router)# neighbor 2018::1 peer-group group1
```

Related Commands

N/A

7.6.44 neighbor peer-group (creating a peer-group)

Command Purpose

Use this command to create a peer-group.

Use the no parameter with this command to disable this function

Command Syntax

```
neighbor TAG peer-group
no neighbor TAG peer-group
```

Parameter	Parameter Description	Parameter Value
TAG	Name of the peer-group	-

Command Mode

Router Configuration

Default

N/A

Usage

Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor group1 peer-group
```

Related Commands

N/A

7.6.45 neighbor prefix-list

Command Purpose

Use this command to distribute BGP neighbor information as specified in a prefix list.
Use the no parameter with this command to remove an entry.

Command Syntax

```
neighbor NEIGHBORID prefix-list LISTNAME ( in | out )
no neighbor NEIGHBORID prefix-list LISTNAME ( in | out )
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
LISTNAME	The number of an AS-path access list.	Up to 20 characters
in	Specifies that the access list applies to incoming advertisements.	-
out	Specifies that the access list applies to outgoing advertisements.	-

Command Mode

Address Family Configuration

Default

N/A

Usage

Use this command to specify a prefix list for filtering BGP advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top. The neighbor distribute-list command is an alternative to the neighbor prefix-list command and only one of them can be used for filtering to the same neighbor in any direction.

Examples

```
Switch# configure terminal
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 10.10.10.10 prefix-list list1 in
```

Related Commands

ip prefix-list

7.6.46 neighbor remote-as

Command Purpose

Use this command to configure an internal or external BGP (iBGP or eBGP) TCP session with another router.

Command Syntax

```
neighbor NEIGHBORID remote-as ASNUM
no neighbor NEIGHBORID remote-as ASNUM
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
ASNUM	Neighbor's autonomous system number	1-4294967295

Command Mode

Router Configuration

Default

N/A

Usage

This command is used to configure iBGP and eBGP sessions with other neighbors. A peer-group support of this command is configured only after creating a specific peer-group.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# neighbor 2018::1 remote-as 345
```


Related Commands

N/A

7.6.47 neighbor remove-private-AS

Command Purpose

Use this command to remove the private Autonomous System (AS) number from outbound updates. Use the no parameter with this command too revert to default.

Command Syntax

neighbor *NEIGHBORID* remove-private-AS
no neighbor *NEIGHBORID* remove-private-AS

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Address Family Configuration

Default

Disabled

Usage

The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 remove-private-AS
```

Related Commands

N/A

7.6.48 neighbor route-reflector-client

Command Purpose

Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client. Use the no parameter with this command to indicate that the neighbor is not a client.

Command Syntax

neighbor *NEIGHBORID* route-reflector-client
no neighbor *NEIGHBORID* route-reflector-client

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-

Parameter	Parameter Description	Parameter Value
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Address Family Configuration

Default

N/A

Usage

Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the neighbor route-reflector-client command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 route-reflector-client
```

Related Commands

N/A

7.6.49 neighbor send-community

Command Purpose

Use this command to specify that a community attribute should be sent to a BGP neighbor.

Use the no parameter with this command to remove the entry. Use the extended and no parameters to remove extended communities. Specifying no other parameter means standard communities only.

Command Syntax

```
neighbor NEIGHBORID send-community ( both | extended | standard | )
no neighbor NEIGHBORID send-community ( both | extended | standard | )
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
	both	Sends Standard and Extended Community attributes
	extended	Sends Extended Community attributes
	standard	Sends Standard Community attributes

Command Mode

Address Family Configuration

Default

None

Usage

By default ,community attributes are not sent to a neighbor. To use this command to enable this command.Route-map can be based on neighbor address, peer group name or AS path information.

Examples

```
Switch# configure terminal
Switch(config)# bgp config-type standard
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 send-community extended
```

Related Commands

N/A

7.6.50 neighbor shutdown

Command Purpose

Use this command to disable a neighbor.
Use the no parameter with this command to re-enable the neighbor.

Command Syntax

neighbor *NEIGHBORID* shutdown
no neighbor *NEIGHBORID* shutdown

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
A.B.C.D	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address

Parameter	Parameter Description	Parameter Value
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration

Default

N/A

Usage

This command shuts down any active session for the specified neighbor and clears all related routing data.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 shutdown
```

Related Commands

N/A

7.6.51 neighbor soft-reconfiguration inbound

Command Purpose

Use this command to configure to start storing updates.
Use the no parameter with this command to disable this function.

Command Syntax

neighbor *NEIGHBORID* soft-reconfiguration inbound
no neighbor *NEIGHBORID* soft-reconfiguration inbound

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv4 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration
Address Family Configuration

Default

N/A

Usage

Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 soft-reconfiguration inbound
```

Related Commands

N/A

7.6.52 neighbor strict-capability-match

Command Purpose

Use this command to close the BGP connection if capability value does not completely match to remote peer.
Use the no parameter with this command to disable this function

Command Syntax

```
neighbor NEIGHBORID strict-capability-match
no neighbor NEIGHBORID strict-capability-match
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters

Command Mode

Router Configuration
Default

N/A

Usage

N/A

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 strict-capability-match
```

Related Commands

N/A

7.6.53 neighbor timers

Command Purpose

Use this command to set the timers for a specific BGP neighbor.
Use the no parameter with this command to clear the timers for a specific BGP neighbor

Command Syntax

neighbor *NEIGHBORID* timers *KEEPALIVE* *HOLDTIME*
no neighbor *NEIGHBORID* timers

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
KEEPALIVE	holdtime Frequency (in seconds) at which a router sends keepalive messages to its neighbor. The default is 60 seconds.	1-65535
HOLDTIME	Interval (in seconds) after which, on not receiving a keepalive message, the router declares a neighbor dead. The default is 180 seconds.	3-65535

Command Mode

Router Configuration

Default

N/A

Usage

Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive a message for this period it declares the neighbor dead.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 timers 60 120
```

Related Commands

N/A

7.6.54 neighbor unsuppress-map

Command Purpose

Use this command to selectively leak more-specific routes to a particular neighbor.

Command Syntax

```
neighbor NEIGHBORID unsuppress-map WORD
no neighbor NEIGHBORID unsuppress-map WORD
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X:X::X:X TAG)	-
X:X::X:X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
WORD	Name of route map	-

Command Mode

Address Family Configuration

Default

N/A

Usage

When the aggregate-address command is used with the summary-only option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the unsuppress-map command to selectively leak more-specific routes to a particular neighbor.

Examples

```
Switch# configure terminal
Switch(config)#router bgp 10
Switch(config-router)#address-family ipv6
Switch(config-router-af)#neighbor 2018::1 unsuppress-map mymap
```

Related Commands

N/A

7.6.55 neighbor update-source

Command Purpose

Use this command to allow internal BGP sessions to use any operational interface for TCP connections.
Use the no parameter with this command to restore the interface assignment to the closest interface.

Command Syntax

```
neighbor NEIGHBORID update-source IFNAME
no neighbor NEIGHBORID update-source
```

Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
IFNAME	Specifies the loopback interface.	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Router Configuration

Default

N/A

Usage

Use this command in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# neighbor 2018::1 update-source eth-0-1
```

Related Commands

N/A

7.6.56 neighbor weight

Command Purpose

Use this command to set default weights for routes from this neighbor.
Use the no parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor NEIGHBORID weight WEIGHT
no neighbor NEIGHBORID weight
```


Parameter	Parameter Description	Parameter Value
NEIGHBORID	(X::X::X TAG)	-
X::X::X	Specifies the address of the BGP neighbor in IPv6 format.	IPv6 Address
TAG	Name of an existing peer-group. For information on how to create peer groups, refer to the neighbor peer-group and neighbor remote-as commands. When this parameter is used with a command, the command applies on all peers in the specified group.	Up to 20 characters
WEIGHT	Specifies the weight this command assigns to the route.	0-65535

Command Mode

Address Family Configuration

Default

N/A

Usage

Use this command to specify a weight value to all routes learned from a neighbor. The route with the highest weight gets preference when there are other routes on the network.

Unlike the local-preference attribute, the weight attribute is relevant only to the local router.

The weights assigned using the set weight command overrides the weights assigned using this command.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)# address-family ipv6
Switch(config-router-af)# neighbor 2018::1 weight 60
```

Related Commands

N/A

7.6.57 network**Command Purpose**

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the no form of this command to remove a network route entry.

Command Syntax

```
network X::X::X/M
network X::X::X/M route-map WORD
no network X::X::X/M
no network X::X::X/M route-map WORD
```

Parameter	Parameter Description	Parameter Value
X:X::X:X/M	IPv6 prefix <network>, e.g., 2018::	IPv6 address with mask length
WORD	Name of the route map	The length of route-map name should not greater than 20 and the first character should be 'a'-'z', 'A'-'Z' or '0'-'9'.

Command Mode

Address Family Configuration

Default

N/A

Usage

N/A

Examples

The following example illustrates a address configured as a network route. The network prefix mask length of 64 will be internally derived, that is, 2018::/64:

```
Switch# configure terminal
Switch(config)#router bgp 1
Switch(config-router)#address-family ipv6
Switch(config-router-af)#network 2018::/64
```

```
!
router bgp 1
no synchronization
network 2018::/64
!
```

Related Commands

N/A

7.6.58 network synchronization**Command Purpose**

Use this command to ensure the exact same static network prefix, specified through any of the network commands, is local or has IGP reachability (in the NSM RIB) before being introduced into the BGP RIB.

Use the no parameter with this command to disable this function.

Command Syntax

```
network synchronization
no network synchronization
```

Command Mode

Router Configuration
Address Family Configuration

Default

Network synchronization is disabled by default.

Usage

N/A

Examples

The following example enables IGP synchronization of BGP static network routes in the router configuration mode:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config-router)# network synchronization
```

Related Commands

N/A

7.6.59 synchronization

Command Purpose

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.
Use the no parameter with this command to disable this function.

Command Syntax

```
synchronization
no synchronization
```

Command Mode

Router Configuration
Address Family Configuration

Default

IGP synchronization is disabled.

Usage

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems. The no synchronization command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

Examples

The following example enables IGP synchronization of BGP static network routes in the IPv6-Unicast address family:

```
Switch# configure terminal
Switch(config)# router bgp 11
Switch(config)# address-family ipv6
Switch(config-af)# network synchronization
```

Related Commands

N/A

7.6.60 router bgp

Command Purpose

Use this command to configure a BGP routing process.
Use the no parameter with this command to disable a routing process.

Command Syntax

```
router bgp ASN
no router bgp ASN
```

Parameter	Parameter Description	Parameter Value
ASN	Specifies the Autonomous System (AS) number	1-4294967295

Command Mode

Global Configuration

Default

N/A

Usage

The router bgp command enables a BGP routing process.

Examples

```
Switch# configure terminal
Switch(config)# router bgp 12
Switch(config-router)#
```

Related Commands

N/A

7.6.61 show debugging bgp

Command Purpose

Use this command to display the BGP debugging option set.

Command Syntax

show debugging bgp

Command Mode

Privileged EXEC

Default

N/A

Usage

None

Examples

```
Switch# show debugging bgp
```

Related Commands

N/A

7.6.62 show bgp ipv6

Command Purpose

Use this command to display BGP network information.

Command Syntax

show bgp ipv6 (*IPADDRESS* |)

Parameter	Parameter Description	Parameter Value
IPADDRESS	X:X::X:X X:X::X/M Specifies the address and length.	IPv6 address with mask length
unicast	Specifies a IPv4 unicast address family. This is the default option.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6
```

Related Commands

N/A

7.6.63 show bgp ipv6 community

Command Purpose

Use this command to display routes matching the communities.

Command Syntax

```
show bgp ( ipv6 ) community [ AA:NN | local-AS | no-advertise | no-export ] ( exact-match | )
```

Parameter	Parameter Description	Parameter Value
local-AS	Do not send outside local AS (well-known community).	-
AA:NN	Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format.	Support 2 bytes AS number and 2 bytes community ID
no-advertise	Do not advertise to any peer (well-known community).	-
no-export	Do not export to next AS (well-known community).	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 community
Switch# show bgp ipv6 community local-AS 100
```

Related Commands

N/A

7.6.64 show bgp ipv6 community-list

Command Purpose

Use this command to display routes that match the community-list.

Command Syntax

show ip bgp community-list *LISTNAME* (exact-match |)

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the community list name.	Up to 20 characters
exact-match	Displays only routes that have exactly the same specified communities.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 community-list mylist exact-match
Switch# show bgp ipv6 unicast community-list mylist
```

Related Commands

N/A

7.6.65 show bgp ipv6 dampening

Command Purpose

Use this command to display detailed information about dampening.

Command Syntax

show bgp ipv6 dampening (dampened-paths | flap-statistics | parameters)

Parameter	Parameter Description	Parameter Value
dampened-paths	Display paths suppressed due to dampening.	-
flap-statistics	Display flap statistics of routes.	-
parameters	Display details of configured dampening parameters.	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Enable bgp dampening to maintain dampened-path information in memory. The following is a sample output displaying all the dampening parameters:

```
Switch# show bgp ipv6 dampening parameters
```

Related Commands

N/A

7.6.66 show bgp ipv6 filter-list**Command Purpose**

Use this command to display routes conforming to the filter-list.

Command Syntax

```
show ip bgp filter-list LISTNAME
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specifies the access list name.	Up to 20 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 filter-list mylist
```

Related Commands

N/A

7.6.67 show bgp ipv6 inconsistent-as**Command Purpose**

Use this command to display routes with inconsistent AS Paths.

Command Syntax

```
show bgp ipv6 inconsistent-as
```

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 inconsistent-as
```

Related Commands

N/A

7.6.68 show bgp ipv6 neighbors

Command Purpose

Use this command to display detailed information on TCP and BGP neighbor connections.

Command Syntax

show bgp ipv6 neighbors (*IPv6_ADDR* |)

Parameter	Parameter Description	Parameter Value
IPv6_ADDR	X::X::X Specifies the IPv6 address.	IPv6 Address

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show bgp ipv6 neighbors command displaying information about the specified neighbor:
Switch# show bgp ipv6 neighbors

Related Commands

N/A

7.6.69 show bgp ipv6 paths

Command Purpose

Use this command to display BGP path information.

Command Syntax

show bgp ipv6 paths

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

Switch# show bgp ipv6 paths

Related Commands

N/A

7.6.70 show bgp ipv6 prefix-list

Command Purpose

Use this command to display routes matching the prefix-list.

Command Syntax

show bgp ipv6 prefix-list *LIST*

Parameter	Parameter Description	Parameter Value
LIST	Specifies the name of the IPv6 prefix list.	Up to 40 characters

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 prefix-list mylist
```

Related Commands

N/A

7.6.71 show bgp ipv6 quote-regexp

Command Purpose

Use this command to display routes matching the AS path regular expression in quotes.

Command Syntax

show bgp ipv6 quote-regexp *WORD*

Parameter	Parameter Description	Parameter Value
WORD	Specifies a regular-expression to match the BGP AS paths	Regular expression in quotes

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 quote-regexp "Switch"
```

Related Commands

N/A

7.6.72 show bgp ipv6 regexp

Command Purpose

Use this command to display routes matching the AS path regular expression.

Command Syntax

show bgp ipv6 regexp *LINE*

Parameter	Parameter Description	Parameter Value
<i>LINE</i>	Displays routes matching the AS path regular expression.	Regular expression

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

```
Switch# show bgp ipv6 regexp myexpression
```

Related Commands

N/A

7.6.73 show bgp ipv6 summary

Command Purpose

Use this command to display a summary of BGP neighbor status.

Command Syntax

show bgp ipv6 summary

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This is a sample output from the show bgp ipv6 summary command displaying a summary of BGP neighbor status:
Switch# show bgp ipv6 summary

Related Commands

N/A

7.6.74 timers

Command Purpose

Use this command sets the BGP keepalive timer and holdtime timer values.
Use the no parameter with this command to reset timers to default value.

Command Syntax

```
timers bgp KEEPALIVE HOLDTIME  
no timers bgp
```

Parameter	Parameter Description	Parameter Value
KEEPALIVE	<0-65535> The frequency with which the keepalive messages are sent to the neighbors. The default value is 60 seconds.	0-65535
HOLDTIME	The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 180 seconds.	3-65535

Command Mode

Router Configuration

Default

N/A

Usage

This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

Examples

```
Switch# configure terminal  
Switch(config)# router bgp 10  
Switch(config-router)# timers bgp 40 120
```

Related Commands

N/A

Chapter 8 Multicast Commands

8.1 IP Multicast-Routing Commands

8.1.1 ip multicast-routing

Command Purpose

Use this command to enable ip multicast routing.
To disable ip multicast routing, use the no form of this command.

Command Syntax

```
ip multicast-routing
no ip multicast-routing
```

Command Mode

Global Configuration

Default

Enable

Usage

None

Examples

This example shows how to enable ip multicast routing:

```
Switch# configure terminal
```

```
Switch(config)# ip multicast-routing
```

This example shows how to disable ip multicast routing:

```
Switch# configure terminal
```

```
Switch(config)# no ip multicast-routing
```

Related Commands

None

8.1.2 ip multicast route-limit

Command Purpose

Use this command to set the maximum number of the multicast routes.
To return it to default value, use the no form of this command.

Command Syntax

```
ip multicast route-limit ROUTE_NUMBER ( THRESHOLD_NUMBER | )
no ip multicast route-limit
```

Parameter	Parameter Description	Parameter Value
ROUTE_NUMBER	Max number of multicast route entries	1-2048
THRESHOLD_NUMBER	Threshold at which to generate warning message	1-2048

Command Mode

Global Configuration

Default

Default maximum number of the multicast routes is 2048.
Default threshold is same as the maximum number of multicast routes.

Usage

None

Examples

This example shows how to set the maximum number of the multicast routes to 512:

```
Switch# configure terminal
Switch(config)# ip multicast route-limit 512
```

This example shows how to return the maximum number of the multicast routes to default value:

```
Switch# configure terminal
Switch(config)# no ip multicast route-limit
```

Related Commands

show ip mroute route-limit

8.1.3 show ip mroute

Command Purpose

Use this command to display the ip multicast routing table information.

Command Syntax

```
show ip mroute ( sparse | ) ( count | summary | )
show ip mroute IP_ADDR ( sparse | ) ( count | summary | )
show ip mroute route-limit
```

Parameter	Parameter Description	Parameter Value
sparse	Show sparse multicast routes	-
count	Show number of multicast route entries	-
summary	Show abbreviated multicast route information	-
IP_ADDR	Show specify source or group address multicast route	IPv4 Address
route-limit	Show max route limit value	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast routing table:

```
Switch# 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)
```

```
(10.0.1.20, 228.1.1.1), uptime 00:35:46, stat expires 00:02:19
```

```
Owner PIM-SM, Flags: TF
```

```
Incoming interface: eth-0-1
```

```
Outgoing interface list:
eth-0-2 (1)
```

This example shows how to display multicast routing table summary information:

```
Switch# 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)
```

```
(10.0.1.20, 228.1.1.1), 00:36:59/00:02:46, PIM-SM, Flags: TF
```

Related Commands

```
ip multicast route-limit
```

```
ip mroute-rpf
```

8.1.4 show ip mvif

Command Purpose

Use this command to display the multicast interface information.

Command Syntax

```
show ip mvif ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast interface information:

```
Switch# show ip mvif
```

Interface	Vif Idx	Owner Module	TTL	Local Address	Remote Address	Uptime
eth-0-1	0	PIM-SM	1	10.0.1.1	0.0.0.0	00:42:56
eth-0-2	2	PIM-SM	1	10.0.2.1	0.0.0.0	00:42:53

Related Commands

```
ip pim sparse-mode
```

8.1.5 show ip multicast groups count

Command Purpose

Use this command to display the multicast group count.

Command Syntax

show ip multicast groups count

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast group number:

```
Switch# show ip multicast groups count
```

```
multicast group record count: 1
multicast source record count: 0
multicast total record count: 1
multicast max record count: 2048
```

Related Commands

None

8.1.6 show resource mcast

Command Purpose

Use this command to display multicast resource information.

Command Syntax

show resource mcast

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast resource information:

```
Switch# show resource mcast
```

MCAST Resource	Used	Capability
Mcast Entry	0	1023
Mcast Normal Member	0	2046
Mcast Vlan Member	0	1023

Related Commands

None

8.1.7 clear ip mroute

Command Purpose

Use this command to clear the multicast routing table information.

Command Syntax

```
clear ip mroute ( * | GRP_ADDR ( SRC_IP ) | )
```

Parameter	Parameter Description	Parameter Value
GRP_ADDR	Clear specify group address multicast route	IPv4 Address
SRC_ADDR	Clear specify source address multicast route	IPv4 Address
*	Clear all multicast routes	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all multicast routing table information:

```
Switch# clear ip mroute *
```

Related Commands

```
show ip mroute
```

8.2 IGMP Commands

8.2.1 ip igmp access-group

Command Purpose

Use this command to apply an access-list to the igmp interface.
To remove this setting, use the no form of this command.

Command Syntax

```
ip igmp access-group LIST  
no ip igmp access-group
```

Parameter	Parameter Description	Parameter Value
LIST	The name of the ip access-list to be applied. The format of access-list should be ipv4.	Up to 40 characters

Command Mode

Interface Configuration

Default

Access-group is not configured on any igmp interface by default.

Usage

No matter the source ip or the destination ip in ACE should take effect respectively. If ACE's action is deny, then the packet should be ignored; otherwise, if it matches one whose action is permit, then it should be processed regularly.

Examples

This example shows how to apply the access-list acl1 to the interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp access-group acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp access-group
```

Related Commands

show ip igmp interface

8.2.2 ip igmp immediate-leave group-list

Command Purpose

Use this command to apply an access-list to configure which groups support immediate-leave per interface. To remove this setting, use the no form of this command.

Command Syntax

```
ip igmp immediate-leave group-list LIST
no ip igmp immediate-leave
```

Parameter	Parameter Description	Parameter Value
LIST	The name of the ip access-list to be applied. The format of access-list should be ipv4.	Up to 40 characters

Command Mode

Interface Configuration

Default

Access-group is not configured on any igmp interface by default.

Usage

No matter the source ip or the destination ip in ACE should take effect respectively. If ACE's action is deny, then the packet should be ignored; Otherwise if it matches one whose action is permit, then it should be processed regularly.

Examples

This example shows how to apply an access-list to configure which groups support immediately-leave on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp immediate-leave group-list acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp immediate-leave group-list
```

Related Commands

show ip igmp interface

8.2.3 ip igmp last-member-query-count

Command Purpose

Use this command to set the value of last member query count.

To reset it to default value, use the no form of this command.

Command Syntax

ip igmp last-member-query-count *COUNT*
no ip igmp last-member-query-count

Parameter	Parameter Description	Parameter Value
COUNT	The value of last member query count	2-7

Command Mode

Interface Configuration

Default

2

Usage

None

Examples

This example shows how to set the value of last member query count to 5:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp last-member-query-count 5
```

This example shows how to reset the value of last member query count to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp last-member-query-count
```

Related Commands

show ip igmp interface

ip igmp last-member-query-interval

8.2.4 ip igmp last-member-query-interval

Command Purpose

Use this command to set the value of last member query interval.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp last-member-query-interval *INTERVAL*
no ip igmp last-member-query-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	The last member query interval value(ms)	1000-25500 ms

Command Mode

Interface Configuration

Default

1000ms

Usage

None

Examples

This example shows how to set the last member query interval value to 10000ms:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp last-member-query-interval 10000
```

This example shows how to reset the last member query interval value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp last-member-query-interval
```

Related Commands

```
show ip igmp interface
ip igmp last-member-query-count
```

8.2.5 ip igmp limit

Command Purpose

Use this command to set the max num of groups allowed.
To reset it to default value, use the no form of this command.

Command Syntax

```
ip igmp limit NUMBER except LIST
no ip igmp limit
```

Parameter	Parameter Description	Parameter Value
NUMBER	The max num of groups	1-2048
LIST	Groups not to be counted	

Command Mode

Global Configuration & Interface Configuration

Default

2048

Usage

Max number of groups is 2048 by default,in global configuration mode, use this command to set number of groups for all ports, in interface configuration mode, use this command to set number of groups for one ports

Examples

This example shows how to set the max num of groups allowed to 1000 globally:

```
Switch# configure terminal
Switch(config)# ip igmp limit 1000
```

This example shows how to reset the max num of groups to default value:

```
Switch# configure terminal
Switch(config)# no ip igmp limit
```

Related Commands

```
show ip igmp interface
```

8.2.6 ip igmp mroute-proxy

Command Purpose

Use this command to set the mroute-proxy port on this interface.
To remove it, use the no form of this command.

Command Syntax

```
ip igmp mroute-proxy IFNAME
no ip igmp mroute-proxy
```

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name of the mroute-proxy port	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Interface Configuration

Default

None

Usage

This command is used to set the mroute-proxy port on the interface. Only one mroute-proxy port can be set on the interface. When set it again, the new setting will overwrite the old one.

Examples

This example shows how to set the mroute-proxy port to eth-0-1 on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp mroute-proxy eth-0-1
```

This example shows how to remove the mroute-proxy port on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp mroute-proxy
```

Related Commands

ip igmp proxy-service

8.2.7 ip igmp proxy-service

Command Purpose

Use this command to enable igmp mroute proxy service on the interface. To disable it, use the no form of this command

Command Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Command Mode

Interface Configuration

Default

None

Usage

This command is used with command ip igmp mroute-proxy and to set the upstream interface of the igmp group.

Examples

This example shows how to enable igmp mroute proxy service on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp proxy-service
```

This example shows how to disable igmp mroute proxy service:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp proxy-service
```

Related Commands

ip igmp mroute-proxy

8.2.8 ip igmp querier-timeout

Command Purpose

Use this command to set the igmp previous querier timeout value.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp querier-timeout *INTERVAL*
no ip igmp querier-timeout

Parameter	Parameter Description	Parameter Value
INTERVAL	The igmp previous querier timeout value	60-300 seconds

Command Mode

Interface Configuration

Default

255s

Usage

None

Examples

This example shows how to set the igmp previous querier timeout value to 100 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp querier-timeout 100
```

This example shows how to reset the igmp previous querier timeout value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if) #no ip igmp querier-timeout
```

Related Commands

ip igmp query-interval
ip igmp query-max-response-time

8.2.9 ip igmp query-interval

Command Purpose

Use this command to set the igmp query interval.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp query-interval *INTERVAL*
no ip igmp query-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	The value of igmp query interval	2-18000

Command Mode

Interface Configuration

Default

125s

Usage

None

Examples

This example shows how to set the igmp query interval to 300 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-interval 300
```

This example shows how to reset the igmp query interval to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp query-interval
```

Related Commands

ip igmp querier-timeout
ip igmp query-max-response-time

8.2.10 ip igmp query-max-response-time

Command Purpose

Use this command to set the igmp query max response time.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp query-max-response-time *INTERVAL*
no ip query-max-response-time

Parameter	Parameter Description	Parameter Value
INTERVAL	The igmp query max response time	1-25

Command Mode

Interface Configuration

Default

10 seconds

Usage

Query max response time must be less than igmp query interval.

Examples

This example shows how to set the igmp query max response time to 20 seconds.:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-max-response-time 20
```

This example shows how to reset the igmp query max response time to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp query-max-response-time
```

Related Commands

ip igmp querier-timeout
ip igmp query-interval

8.2.11 ip igmp robustness-variable

Command Purpose

Use this command to set the igmp querier robustness variable value.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp robustness-variable *VALUE*
no ip robustness-variable

Parameter	Parameter Description	Parameter Value
VALUE	The igmp querier robustness variable value	2-7

Command Mode

Interface Configuration

Default

2

Usage

None

Examples

This example shows how to set the igmp querier robustness variable value to 6:

```
Switch# configure terminal
```

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ip igmp robustness-variable 6
```

This example shows how to reset the igmp querier robustness variable value to default value:

```
Switch# configure terminal
```

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# no ip igmp robustness-variable
```

Related Commands

show ip igmp interface

8.2.12 ip igmp version

Command Purpose

Use this command to set the igmp version on interface.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp version *VER*
no ip igmp version

Parameter	Parameter Description	Parameter Value
VER	The igmp version on the interface	1-3

Command Mode

Interface Configuration

Default

2

Usage

None

Examples

This example shows how to set the igmp version 1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp version 1
This example shows how to reset the igmp version to default value:
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp version
```

Related Commands

show ip igmp interface

8.2.13 ip igmp static-group

Command Purpose

Use this command to configure the static multicast group on interface.
To delete static group, use the no form of this command.

Command Syntax

```
ip igmp static-group GRP_ADDR ( source SRC_ADDR | )
no ip igmp static-group GRP_ADDR ( source SRC_ADDR | )
```

Parameter	Parameter Description	Parameter Value
GRP_ADDR	The multicast group address	IPv4 Address
SRC_ADDR	The multicast source address	IPv4 Address

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure the static IGMP group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip igmp static-group 226.1.2.3
Switch(config-if)# ip igmp static-group 226.1.2.4 source 1.2.3.4
```

This example shows how to delete static igmp group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ip igmp static-group 226.1.2.3
```

Related Commands

show ip igmp groups

8.2.14 ip igmp ssm-map enable

Command Purpose

Use this command to enable igmp ssm mapping.
To disable ssm mapping, use the no form of this command.

Command Syntax

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```


Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable igmp ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp ssm-map enable
```

This example shows how to disable igmp ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp ssm-map enable
```

Related Commands

None

8.2.15 ip igmp ssm-map static**Command Purpose**

Use this command to set igmp ssm mapping.

To cancel ssm mapping setting, use the no form of this command.

Command Syntax

```
ip igmp ssm-map static LIST SRC_ADDR
```

```
no ip igmp ssm-map static LIST SRC_ADDR
```

Parameter	Parameter Description	Parameter Value
LIST	Specify multicast group address range access list	Up to 40 characters
SRC_ADDR	Multicast source address	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set igmp ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp ssm-map static ipacl 192.168.1.1
```

This example shows how to unset igmp ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp ssm-map static ipacl 192.168.1.1
```

Related Commands

None

8.2.16 clear ip igmp**Command Purpose**

Use this command to clear igmp groups.

Command Syntax

clear ip igmp group (* | *GRP_ADDR* |)

Parameter	Parameter Description	Parameter Value
*	All multicast group address	-
GRP_ADDR	Multicast group address	IPv4 Address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear igmp group all:

```
Switch# clear ip igmp
```

```
Switch# clear ip igmp group *
```

This example shows how to clear igmp specified group:

```
Switch# clear ip igmp group 228.1.1.1
```

Related Commands

show ip igmp groups

8.2.17 clear ip igmp interface

Command Purpose

Use this command to clear igmp groups on specified interface.

Command Syntax

clear ip igmp interface *IFNAME*

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear igmp group on specified interface:

```
Switch# clear ip igmp group interface eth-0/1
```

Related Commands

show ip igmp groups

8.2.18 show ip igmp groups

Command Purpose

Use this command to show the information about igmp groups.

Command Syntax

show ip igmp groups *GRP_ADDR* (detail |)

Parameter	Parameter Description	Parameter Value
GRP_ADDR	Specify multicast group address	IPv4 Address
detail	Detailed Information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the detail information about igmp groups:

Switch# show ip igmp groups detail

```
Interface:      eth-0-1
Group:          227.0.0.1
Uptime:         00:00:33
Group mode:     Exclude (Expires: 00:04:18)
Last reporter:  10.0.1.100
Source list is empty
```

Related Commands

None

8.2.19 show ip igmp groups interface

Command Purpose

Use this command to show the information about igmp groups on interface.

Command Syntax

show ip igmp groups *IFNAME* (*GRP_ADDR* |) (detail |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports
GRP_ADDR	Specify multicast group address	IPv4 Address
detail	Detailed Information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about igmp groups on interface eth-0-1:

```
Switch# show ip igmp groups eth-0-1
```

```
IGMP Connected Group Membership
Group Address    Interface    Uptime    Expires    Last Reporter
227.0.0.1        eth-0-1      00:01:11  00:04:16  10.0.1.100
```

Related Commands

None

8.2.20 show ip igmp groups count**Command Purpose**

Use this command to show igmp group number.

Command Syntax

```
show ip igmp groups ( IFNAME | ) count
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the igmp group number on interface eth-0-1:

```
Switch# show ip igmp groups eth-0-1 count
```

```
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

Related Commands

None

8.2.21 show ip igmp interface**Command Purpose**

Use this command to show the information about igmp on interface.

Command Syntax

show ip igmp interface (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about igmp on interface eth-0-1:
Switch# show ip igmp interface eth-0-1

```
Interface eth-0-1 (Index 1)
IGMP Enabled, Active, Querier, Version 2 (default)
Internet address is 10.0.1.1
IGMP interface limit is 8192
IGMP interface has 1 group-record states
IGMP activity: 97 joins, 0 leaves
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
Last memeber query count is 2
Robustness Variable is 2
```

Related Commands

None

8.3 IGMP Snooping Commands

8.3.1 ip igmp snooping

Command Purpose

Use this command to enable igmp snooping.
To disable igmp snooping, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | )
no ip igmp snooping ( vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Enable

Usage

Igmp Snooping can be enabled globally and per vlan. By default, igmp snooping is enabled globally and per vlan.

Examples

This example shows how to enable igmp snooping:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping
```

This example shows how to disable igmp snooping:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping
```

This example shows how to enable igmp snooping on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 10
```

This example shows how to disable igmp snooping on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping vlan 10
```

Related Commands

```
show ip igmp snooping
```

8.3.2 ip igmp snooping fast-leave

Command Purpose

Use this command to enable igmp snooping fast leave.
To disable it, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) fast-leave
```

```
no ip igmp snooping ( vlan VLAN_ID | ) fast-leave
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

This command will override immediate-leave setting.

Examples

This example shows how to enable igmp snooping fast-leave:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping fast-leave
```

This example shows how to disable igmp snooping fast-leave:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping fast-leave
```

Related Commands

```
show ip igmp snooping global
```

8.3.3 ip igmp snooping last-member-query-interval

Command Purpose

Use this command to set the last member query interval of igmp snooping.
To reset it to default value, use the no form of this command.

Command Syntax

ip igmp snooping (vlan *VLAN_ID* |) last-member-query-interval *INTERVAL*
no ip igmp snooping (vlan *VLAN_ID* |) last-member-query-interval

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The last member query interval	1000-25500 ms

Command Mode

Global Configuration

Default

1000 ms

Usage

Igmp last member query interval can be configured per vlan. The default is 1000ms and the range is 1000-25500ms.

Examples

This example shows how to set the last member query interval:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

This example shows how to reset the last member query interval to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping last-member-query-interval
```

Related Commands

```
show ip igmp snooping
```

```
show ip igmp snooping vlan
```

8.3.4 ip igmp snooping global source-address

Command Purpose

Use this command to set the global source address.

To reset it to default value, use the no form of this command.

Command Syntax

ip igmp snooping global source-address *IP_ADDR*

no ip igmp snooping global source-address

Parameter	Parameter Description	Parameter Value
IP_ADDR	The IPv4 address of source address	IPv4 Address

Command Mode

Global Configuration

Default

0.0.0.0

Usage

Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples

This example shows how to set the global source address to 1.3.4.5:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping global source-address 1.3.4.5
```

This example shows how to reset the global source address to default value:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping global source-address
```

Related Commands

```
show ip igmp snooping querier
```

8.3.5 ip igmp snooping max-member-num

Command Purpose

Use this command to set the max allowed member number.
To reset it to default value, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) max-member-num NUMBER
no ip igmp snooping ( vlan VLAN_ID | ) max-member-num
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
NUMBER	The max member number of igmp snooping	1-2048

Command Mode

Global Configuration

Default

2048

Usage

None

Examples

This example shows how to set the max member number of igmp snooping to 1024:

```
Switch# configure terminal
Switch(config)# ip igmp snooping max-member-num 1024
```

This example shows how to reset the max member number to default value:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping max-member-num
```

Related Commands

```
show ip igmp snooping global
show ip igmp snooping vlan
```

8.3.6 ip igmp snooping query-interval

Command Purpose

Use this command to set the igmp snooping query-interval.
To reset the query-interval to default value, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) query-interval interval
no ip igmp snooping ( vlan VLAN_ID | ) query-interval
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The query-interval of igmp snooping	2-18000 seconds

Command Mode

Global Configuration

Default

125s

Usage

Query interval can not be less than igmp snooping query max response time.

Examples

This example shows how to set the igmp snooping query interval to 64s:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping query-interval 64
```

This example shows how to reset the query-interval to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping query-interval
```

Related Commands

```
show ip igmp snooping querier
```

```
show ip igmp snooping querier vlan
```

8.3.7 ip igmp snooping query-max-response-time

Command Purpose

Use this command to set the igmp snooping query-interval.

To reset the query-interval to default value, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) query-max-response-time TIME
```

```
no ip igmp snooping ( vlan VLAN_ID | ) query-max-response-time
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
TIME	The query max response time in seconds	1-25

Command Mode

Global Configuration

Default

10s

Usage

Query interval can not be less than igmp snooping query max response time.

Examples

This example shows how to set the igmp snooping query max response time to 15s:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping query-max-response-time 15
```

This example shows how to reset the query max response time to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping query-max-response-time
```

Related Commands

```
show ip igmp snooping querier
show ip igmp snooping querier vlan
```

8.3.8 ip igmp snooping report-suppression

Command Purpose

Use this command to enable report suppression.
To disable report suppression, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) report-suppression
no ip igmp snooping ( vlan VLAN_ID | ) report-suppression
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Enable

Usage

Will not do report suppression when IGMP snooping works in v3 mode.

Examples

This example shows how to enable the report suppression:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping report-suppression
```

This example shows how to disable report suppression:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping report-suppression
```

Related Commands

```
show ip igmp snooping
show ip igmp snooping vlan
```

8.3.9 ip igmp snooping version

Command Purpose

Use this command to set igmp snooping version.
To reset it to default value, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) version VER
no ip igmp snooping ( vlan VLAN_ID | ) version
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
VER	Igmp snooping version	1-3

Command Mode

Global Configuration

Default

2

Usage

The default version is 2.

Examples

This example shows how to set the igmp snooping version 1:

```
Switch# configure terminal
Switch(config)# ip igmp snooping version 1
```

Related Commands

```
show ip igmp snooping
show ip igmp snooping vlan
```

8.3.10 ip igmp snooping discard-unknown

Command Purpose

Use this command to set discard unknown multicast traffic.
To disable discard unknown, use the no form of this command.

Command Syntax

```
ip igmp snooping ( vlan VLAN_ID | ) discard-unknown
no ip igmp snooping ( vlan VLAN_ID | ) discard-unknown
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Enabled by default, unknown multicast traffic will flood in vlan.

Usage

None

Examples

This example shows how to enable discard-unknown multicast traffic:

```
Switch# configure terminal
Switch(config)# ip igmp snooping discard-unknown
```

Related Commands

```
show ip igmp snooping
show ip igmp snooping vlan
```

8.3.11 ip igmp snooping querier tcn

Command Purpose

Use this command to set IGMP snooping querier TCN related parameters. To reset it to default value, use the no form of this command.

Command Syntax

```
ip igmp snooping querier tcn ( enable | query-count COUNT | query-interval INTERVAL | query-max-response-time TIME )
no ip igmp snooping querier tcn ( enable | query-count | query-interval | query-max-response-time )
```

Parameter	Parameter Description	Parameter Value
enable	IGMP querier TCN query enable	-
COUNT	IGMP querier TCN query count, default is 2.	1-10
INTERVAL	IGMP querier TCN query interval, default is 10s.	1-255 seconds
TIME	IGMP querier TCN query max response time, default is 5s	1-9 seconds

Command Mode

Global Configuration

Default

This feature is enabled by default, default query count is 2, default query interval is 10s, maximum response time is 5s

Usage

None

Examples

This example shows how to use ip igmp snooping querier tcn command:

```
Switch# configure terminal
Switch(config)# ip igmp snooping querier tcn query-count 2
```

Related Commands

show ip igmp snooping querier

8.3.12 ip igmp snooping vlan access-group

Command Purpose

Use this command to set igmp snooping access group on vlan. To remove this setting, use the no form of this command.

Command Syntax

```
ip igmp snooping vlan VLAN_ID access-group LIST
no ip igmp snooping vlan VLAN_ID access-group
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
LIST	IP Named Standard Access list.	Up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to apply access-group on vlan 10:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 access-group acl
```

This example shows how to remove access-group from vlan 10:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 access-group
```

Related Commands

show ip igmp snooping vlan

8.3.13 ip igmp snooping vlan mrouter interface

Command Purpose

Use this command to set igmp snooping mrouter interface on vlan. To remove this setting, use the no form of this command.

Command Syntax

ip igmp snooping vlan *VLAN_ID* mrouter interface *IFNAME*
no ip igmp snooping vlan *VLAN_ID* mrouter interface *IFNAME*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
IFNAME	Mrouter interface on this vlan	Support physical/aggregation ports

Command Mode

Global Configuration

Default

None

Usage

The specified interface must have already joined the configured vlan.

Examples

This example shows how to set eth-0-1 as mrouter interface on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 10 mrouter interface eth-0-1
```

This example shows how to unset eth-0-1 as mrouter interface on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping vlan 10 mrouter interface eth-0-1
```

Related Commands

show ip igmp snooping vlan

8.3.14 ip igmp snooping vlan mrouter-aging-interval

Command Purpose

Use this command to set igmp snooping mrouter interface aging interval on vlan. To reset it to default value, use the no form of this command.

Command Syntax

ip igmp snooping vlan *VLAN_ID* mrouter-aging-interval *INTERVAL*
no ip igmp snooping vlan *VLAN_ID* mrouter-aging-interval

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	Dynamic mrouter interface aging interval on this vlan in seconds	1-65535 seconds

Command Mode

Global Configuration

Default

255s

Usage

None

Examples

This example shows how to set dynamic mrouter interface aging interval as 100 seconds on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 10 mrouter-aging-interval 100
```

This example shows how to reset dynamic mrouter interface aging interval as default on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping vlan 10 mrouter-aging-interval
```

Related Commands

```
show ip igmp snooping vlan
```

8.3.15 ip igmp snooping vlan querier**Command Purpose**

Use this command to enable igmp snooping querier on vlan. To reset it to default, use the no form of this command.

Command Syntax

```
ip igmp snooping vlan VLAN_ID querier
```

```
no ip igmp snooping vlan VLAN_ID querier
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable querier on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ip igmp snooping vlan 10 querier
```

This example shows how to disable querier on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ip igmp snooping vlan 10 querier
```

Related Commands

```
show ip igmp snooping querier vlan
```

8.3.16 ip igmp snooping vlan querier address**Command Purpose**

Use this command to set igmp snooping querier address on vlan. To remove this setting, use the no form of this command.

Command Syntax

ip igmp snooping vlan *VLAN_ID* querier address *IP_ADDR*
no ip igmp snooping vlan *VLAN_ID* querier address *IP_ADDR*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
IP_ADDR	The address of querier on this vlan	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples

This example shows how to set querier address on vlan 10:

```
Switch# configure terminal  
Switch(config)# ip igmp snooping vlan 10 querier address 1.1.1.1
```

This example shows how to unset querier address on vlan 10:

```
Switch# configure terminal  
Switch(config)# no ip igmp snooping vlan 10 querier address
```

Related Commands

show ip igmp snooping querier vlan

8.3.17 ip igmp snooping vlan querier-timeout

Command Purpose

Use this command to set igmp previous querier timeout interval on this vlan. To reset it to default, use the no form of this command.

Command Syntax

ip igmp snooping vlan *VLAN_ID* querier-timeout *INTERVAL*
no ip igmp snooping vlan *VLAN_ID* querier-timeout

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The igmp previous querier timeout interval on this vlan in seconds	60-300 seconds

Command Mode

Global Configuration

Default

255s

Usage

None

Examples

This example shows how to set previous querier timeout interval as 100 seconds on vlan 10:

```
Switch# configure terminal  
Switch(config)# ip igmp snooping vlan 10 querier-timeout 100
```

This example shows how to reset previous querier timeout interval on vlan 10:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 querier-timeout
```

Related Commands

show ip igmp snooping querier vlan

8.3.18 ip igmp snooping vlan static-group

Command Purpose

Use this command to add static igmp group on this vlan. To remove this setting, use the no form of this command.

Command Syntax

```
ip igmp snooping vlan VLAN_ID static-group GRP_ADDR ( source SRC_ADDR | ) interface IFNAME
no ip igmp snooping vlan VLAN_ID static-group GRP_ADDR ( source SRC_ADDR | ) interface IFNAME
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
GRP_ADDR	The address of group configured on the specified interface.	IPv4 Address
SRC_ADDR	The address of source configured on the specified interface.	IPv4 Address
IFNAME	The interface configured as a member of specified group on this vlan	Support physical/aggregation ports

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to add group 238.1.1.1 on interface eth-0-11 of vlan 10:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 10 static-group 238.1.1.1 interface eth-0-11
```

This example shows how to remove group 238.1.1.1 from interface eth-0-11 of vlan 10:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 10 static-group 238.1.1.1 interface eth-0-11
```

Related Commands

show ip igmp snooping group

8.3.19 clear ip igmp snooping group

Command Purpose

Use this command to clear all igmp snooping groups.

Command Syntax

```
clear ip igmp snooping group ( * | GRP_ADDR )
```


Parameter	Parameter Description	Parameter Value
*	All multicast group address	-
GRP_ADDR	Multicast group address	IPv4 Address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear igmp snooping group all:
 Switch# clear ip igmp snooping group *

Related Commands

None

8.3.20 clear ip igmp snooping vlan**Command Purpose**

Use this command to clear igmp snooping groups on vlan.

Command Syntaxclear ip igmp snooping vlan *VLAN_ID*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear igmp snooping group on vlan 10:
 Switch# clear ip igmp snooping vlan 10

Related Commands

None

8.3.21 show ip igmp snooping global**Command Purpose**

Use this command to show the global configurations of igmp snooping.

Command Syntax

show ip igmp snooping global

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display global configurations of igmp snooping:
Switch# show ip igmp snooping global

Global Igmp Snooping Configuration

Igmp Snooping	:Enabled
Igmp Snooping Fast-Leave	:Disabled
Igmp Snooping Version	:2
Igmp Snooping Robustness Variable	:2
Igmp Snooping Max-Member-Number	:2048
Igmp Snooping Unknown Multicast Behavior	:Flood
Igmp Snooping Report-Suppression	:Enabled

Related Commands

None

8.3.22 show ip igmp snooping groups**Command Purpose**

Use this command to show the igmp snooping groups.

Command Syntax

show ip igmp snooping groups

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display igmp snooping groups:
Switch# show ip igmp snooping groups

VLAN	Interface	Group-Address	Uptime	Expires-time
1	eth-0-1	227.0.0.1	00:03:44	00:04:18

Related Commands

None

8.3.23 show ip igmp snooping groups vlan

Command Purpose

Use this command to show the igmp snooping groups on vlan.

Command Syntax

show ip igmp snooping groups vlan *VLAN_ID* (*GRP_ADDR* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
GRP_ADDR	The address of group	IPv4 Address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display igmp snooping groups on vlan 1:
Switch# show ip igmp snooping groups vlan 1

```
IGMP Snooping groups for vlan1
Interface:      eth-0-1
Group:          227.0.0.1
Uptime:         00:05:24
Group mode:     Exclude (Expires: 00:04:20)
Last reporter:  10.0.1.100
Source list is empty
```

Related Commands

None

8.3.24 show ip igmp snooping groups count

Command Purpose

Use this command to show the igmp snooping groups number.

Command Syntax

show ip igmp snooping groups (vlan *VLAN_ID* |) count

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display igmp snooping groups number on vlan 1:
Switch# show ip igmp snooping groups vlan 1 count

```
Dynamic multicast groups count: 1
Static multicast groups count: 0
Total multicast groups count: 1
```

Related Commands

None

8.3.25 show ip igmp snooping querier

Command Purpose

Use this command to show the configurations of igmp snooping querier information.

Command Syntax

show ip igmp snooping querier (vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the configurations of igmp snooping querier on vlan 1:
Switch# show ip igmp snooping querier vlan 1

Global Igmp Snooping Querier Configuration

```
-----
Version                :2
Last-Member-Query-Interval (msec) :1000
Last-Member-Query-Count      :2
Max-Query-Response-Time (sec)  :10
Query-Interval (sec)         :125
Global Source-Address        :0.0.0.0
TCN Query Count             :2
TCN Query Interval (sec)     :10
TCN Query Max Response Time (sec) :5
Vlan 1:  IGMP snooping querier status
-----
```

Elected querier is : 0.0.0.0

```
-----
Admin state              :Disabled
Admin version            :2
Operational state        :Non-Querier
Querier operational address :0.0.0.0
Querier configure address :N/A
Last-Member-Query-Interval (msec) :1000
Last-Member-Query-Count      :2
Max-Query-Response-Time (sec)  :10
Query-Interval (sec)         :125
Querier-Timeout (sec)       :255
-----
```

Related Commands

None

8.3.26 show ip igmp snooping mrouter**Command Purpose**

Use this command to show the information of igmp snooping mrouter port on vlan.

Command Syntax

show ip igmp snooping mrouter (vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of igmp snooping mrouter port on vlan 1:

```
Switch# show ip igmp snooping mrouter vlan 1
```

Interface	Mode	Uptime	Expires-time
eth-0-11	static	-	-

Related Commands

None

8.3.27 show ip igmp snooping vlan**Command Purpose**

Use this command to show the configurations of igmp snooping on vlan.

Command Syntax

show ip igmp snooping (vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the configurations of igmp snooping on vlan 1:

Switch# show ip igmp snooping vlan 1

Global Igmp Snooping Configuration

```
-----
Igmp Snooping                :Enabled
Igmp Snooping Fast-Leave      :Disabled
Igmp Snooping Version        :2
Igmp Snooping Robustness Variable :2
Igmp Snooping Max-Member-Number :2048
Igmp Snooping Unknown Multicast Behavior :Flood
Igmp Snooping Report-Suppression :Enabled
Vlan 1
-----
```

```
-----
Igmp Snooping                :Enabled
Igmp Snooping Fast-Leave      :Disabled
Igmp Snooping Report-Suppression :Enabled
Igmp Snooping Version        :2
Igmp Snooping Robustness Variable :2
Igmp Snooping Max-Member-Number :2048
Igmp Snooping Unknown Multicast Behavior :Flood
Igmp Snooping Group Access-list :N/A
Igmp Snooping Mrouter Port    :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
-----
```

Related Commands

None

8.3.28 show resource l2mcast

Command Purpose

Use this command to display the resource usage of L2 mcast.

Command Syntax

show resource l2mcast

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource l2mcast command:

Switch# show resource l2mcast

```
L2MCAST
Resource                Used        Capability
=====
L2 Mcast Entry          0          2048
```

Related Commands

None

8.4 PIM Commands

8.4.1 ip pim accept-register

Command Purpose

Use this command to apply an access-list to limit the pim register message received by rp.
To remove this setting, use the no form of this command.

Command Syntax

```
ip pim accept-register list LIST
no ip pim accept-register
```

Parameter	Parameter Description	Parameter Value
LIST	The name of the access-list to be applied.	Up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

This feature is used to prevent the unauthorized user registered to the switch.
When enable this feature, the system will send back a register stop message when the unauthorized register message is received.

Examples

This example shows how to apply the access-list acl1 to limit the pim register message received by rp:

```
Switch# configure terminal
Switch(config)# ip pim accept-register list acl1
```

This example shows how to remove the limits:

```
Switch# configure terminal
Switch(config)# no ip pim accept-register
```

Related Commands

None

8.4.2 ip pim anycast-rp

Command Purpose

Use this command to set anycast rendezvous-point.
To remove the configurations, use the no form of this command.

Command Syntax

```
ip pim anycast-rp ANYCAST_RP_ADDR ANYCAST_MEMBER_ADDR
no ip pim anycast-rp ANYCAST_RP_ADDR ( ANYCAST_MEMBER_ADDR | )
```

Parameter	Parameter Description	Parameter Value
ANYCAST_RP_ADDR	Anycast rp address	IPv4 Address
ANYCAST_MEMBER_ADDR	Anycast member rp address	IPv4 Address

Command Mode

Global Configuration

Default

None.

Usage

Should configure every router in the network, and must configure same RP address.

Examples

This example shows how to set anycast rendezvous-point:

```
Switch# configure terminal
Switch(config)# ip pim anycast-rp 10.10.10.1 10.10.10.11
```

This example shows how to remove the member in anycast rendezvous-point:

```
Switch# configure terminal
Switch(config)# no ip pim anycast-rp 10.10.10.1 10.10.10.11
```

Related Commands

None

8.4.3 ip pim bsr-candidate

Command Purpose

Use this command to configure the candidate bootstrap router (candidate BSR).
To remove the configurations, use the no form of this command.

Command Syntax

```
ip pim bsr-candidate IFNAME ( MASK_LEN ( PRIORITY ) | )
no ip pim bsr-candidate
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support
		physical/aggregation/loopback/vlan/tunnel ports
MASK_LEN	Hash mask length for RP selection	0-32
PRIORITY	Priority value for candidate bootstrap router	0-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to configure the candidate BSR:

```
Switch# configure terminal
Switch(config)# ip pim bsr-candidate eth-0/1
```

This example shows how to cancel the candidate BSR configured:

```
Switch# configure terminal
Switch(config)# no ip pim bsr-candidate
```

Related Commands

ip pim bsr-border

8.4.4 ip pim bsr-border

Command Purpose

Use this command to configure the border of pim domain.
To remove the configurations of the border of pim domain, use the no form of this command.

Command Syntax

```
ip pim bsr-border  
no ip pim bsr-border
```

Command Mode

Interface Configuration

Default

Disable

Usage

None

Examples

This example shows how to configure the border of pim domain:

```
Switch# configure terminal  
Switch(config-if)# ip pim bsr-border
```

This example shows how to remove the configurations of the border of pim domain:

```
Switch# configure terminal  
Switch(config-if)# no ip pim bsr-border
```

Related Commands

```
ip pim bsr-candidate
```

8.4.5 ip pim dr-priority

Command Purpose

Use this command to configure DR priority.
To reset it to default value, use the no form of this command.

Command Syntax

```
ip pim dr-priority PRIORITY  
no ip pim dr-priority
```

Parameter	Parameter Description	Parameter Value
PRIORITY	The DR priority	0-4294967294

Command Mode

Interface Configuration

Default

1

Usage

When a hello message without DR priority is received, it will be regarded to have the max DR priority and to be elected as DR. When more than one router's hello messages do not have DR priority, the one which have the highest ip address will be elected as DR.

Examples

This example shows how to set the pim router DR priority to 1000:

```
Switch# configure terminal  
Switch(config-if)# ip pim dr-priority 1000
```

This example shows how to reset the pim router DR priority to default value:

```
Switch# configure terminal  
Switch(config-if)# no ip pim dr-priority
```

Related Commands

None

8.4.6 ip pim exclude-genid

Command Purpose

Use this command to exclude generation id option from pim hello packets on this interface.
To reset to the default setting, use the no form of this command.

Command Syntax

```
ip pim exclude-genid
no ip pim exclude-genid
```

Command Mode

Interface Configuration

Default

Disable

Usage

GenerationID is the ID of a PIM neighbour, it is carried in PIM hello message, the receiver device will record every received GenerationID in the hello packet and check if GenerationID has changed, if GenerationID changed, will consider neighbour state changed and restart state machine.

Examples

This example shows how to exclude generation id option from pim hello packets on this interface:

```
Switch# configure terminal
```

```
Switch(config-if)# ip pim exclude-genid
```

This example shows how to reset the generation id option to the default setting:

```
Switch# configure terminal
```

```
Switch(config-if)# no ip pim exclude-genid
```

Related Commands

None

8.4.7 ip pim hello-interval

Command Purpose

Use this command to configure the interval for pim hello packets on this interface.
To reset to the default setting, use the no form of this command.

Command Syntax

```
ip pim hello-interval INTERVAL
no ip pim hello-interval
```

Parameter	Parameter Description	Parameter Value
INTERVAL	The pim hello message interval in second	1-18724

Command Mode

Interface Configuration

Default

30s

Usage

None

Examples

This example shows how to set the pim hello message interval to 100s:

```
Switch# configure terminal
```

```
Switch(config-if)# ip pim hello-interval 100
```

This example shows how to reset the pim hello message interval to default value:

```
Switch# configure terminal
```

```
Switch(config-if)# no ip pim hello-interval
```

Related Commands

None

8.4.8 ip pim ignore-rp-set-priority

Command Purpose

Use this command to ignore RP set priority value.

To not ignore the priority, use the no form of this command.

Command Syntax

```
ip pim ignore-rp-set-priority
```

```
no ip pim ignore-rp-set-priority
```

Command Mode

Global Configuration

Default

Not ignore RP set priority value.

Usage

None

Examples

This example shows how to ignore RP set priority value:

```
Switch# configure terminal
```

```
Switch(config)# ip pim ignore-rp-set-priority
```

This example shows how to reset the configurations to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip pim ignore-rp-set-priority
```

Related Commands

None

8.4.9 ip pim jp-timer

Command Purpose

Use this command to set the join/prune timer value.

To reset the timer to default value, use the no form of this command.

Command Syntax

```
ip pim jp-timer TIMER
```

```
no ip pim jp-timer
```

Parameter	Parameter Description	Parameter Value
TIMER	The Join/Prune timer value (second)	1-65535

Command Mode

Global Configuration

Default

60s

Usage

None

Examples

This example shows how to set the join/prune timer value to 100s:

```
Switch# configure terminal
```

```
Switch(config)# ip pim jp-timer 100
```

This example shows how to reset the join/prune timer value to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip pim jp-timer
```

Related Commands

None

8.4.10 ip pim neighbor-filter**Command Purpose**

Use this command to add an access-list to filter the neighbor.

To remove this filter, use the no form of this command.

Command Syntax

```
ip pim neighbor-filter LIST
```

```
no ip pim neighbor-filter
```

Parameter	Parameter Description	Parameter Value
<i>LIST</i>	The name of the access-list	Up to 40 characters

Command Mode

Interface Configuration

Default

None

Usage

Neighbours would send hello message to each other to establish connections with other neighbour, you can use this command to filter which neighbour can be connected or not.

Examples

This example shows how to establish neighbors based on access-list acl1:

```
Switch# configure terminal
```

```
Switch(config-if)# ip pim neighbor-filter acl1
```

This example shows how to cancel the filter:

```
Switch# configure terminal
```

```
Switch(config-if)# no ip pim neighbor-filter
```

Related Commands

None

8.4.11 ip pim register-rate-limit**Command Purpose**

Use this command to set the rate limit for pim registers.

To reset the rate limit to default value, use the no form of this command.

Command Syntax

```
ip pim register-rate-limit LIMIT
no ip pim register-rate-limit
```

Parameter	Parameter Description	Parameter Value
LIMIT	The rate limit for pim registers send from dr to rp	1-65535

Command Mode

Global Configuration

Default

By default, will not limit PIM register messages, if a limit is set, PIM register messages will be discard when pakcet reached by this limit.

Usage

There is no rate limit for pim registers by default.
When the rate limit is configured, the exceed pim register message will be dropped on the rp.

Examples

This example shows how to set the rate limit for pim registers to 100 per second.:

```
Switch# configure terminal
Switch(config)# ip pim register-rate-limit 100
```

This example shows how to cancel the rate limit:

```
Switch# configure terminal
Switch(config)# no ip pim register-rate-limit
```

Related Commands

```
ip pim register-rp-reachability
ip pim register-source
ip pim register-suppression
```

8.4.12 ip pim register-source

Command Purpose

Use this command to set the source address for pim register.
To reset the source address for pim register to default value, use the no form of this command.

Command Syntax

```
ip pim register-source IFNAME
no ip pim register-source
```

Parameter	Parameter Description	Parameter Value
IFNAME	The name of the interface. Use the address of this interface to be the source address for pim register	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Global Configuration

Default

The source address for pim register is the interface ip of dr by default.

Usage

None

Examples

This example shows how to set the source address for pim register to the ip address of interface eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# ip pim register-source eth-0-1
```

This example shows how to reset the source address for pim register to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip pim register-source
```

Related Commands

```
ip pim register-rate-limit
```

```
ip pim register-rp-reachability
```

```
ip pim register-suppression
```

8.4.13 ip pim register-rp-reachability

Command Purpose

Use this command to enable rp reachability check for pim registers.

To disable this check, use the no form of this command.

Command Syntax

```
ip pim register-rp-reachability
```

```
no ip pim register-rp-reachability
```

Command Mode

Global Configuration

Default

Disable.

Usage

None

Examples

This example shows how to enable rp reachability check for pim registers:

```
Switch# configure terminal
```

```
Switch(config)# ip pim register-rp-reachability
```

This example shows how to disable rp reachability check for pim registers:

```
Switch# configure terminal
```

```
Switch(config)# no ip pim register-rp-reachability
```

Related Commands

```
ip pim register-rate-limit
```

```
ip pim register-source
```

```
ip pim register-suppression
```

8.4.14 ip pim register-suppression

Command Purpose

Use this command to set the register suppression time.

To reset this time to default value, use the no form of this command.

Command Syntax

```
ip pim register-suppression TIME
```

```
no ip pim register-suppression
```

Parameter	Parameter Description	Parameter Value
TIME	The register suppression time in seconds	11-18000 seconds

Command Mode

Global Configuration

Default

60s

Usage

None

Examples

This example shows how to set the register suppression time to 100s:

```
Switch# configure terminal
Switch(config)# ip pim register-suppression 100
```

This example shows how to reset the register suppression time to default value:

```
Switch# configure terminal
Switch(config)# no ip pim register-suppression
```

Related Commands

```
ip pim register-rate-limit
ip pim register-rp-reachability
ip pim register-source
```

8.4.15 ip pim rp-address**Command Purpose**

Use this command to set the pim rp (rendezvous point) address.
To remove this setting, use the no form of this command.

Command Syntax

```
ip pim rp-address IP_ADDR ( LIST | override | )
no ip pim rp-address IP_ADDR ( LIST | )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	The rp address	IPv4 Address
LIST	The name of an access-list	Up to 40 characters
override	Overrides dynamically learned RP mappings	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set the pim rp address to 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip pim rp-address 1.1.1.1
This example shows how to remove the rp address 1.1.1.1:
Switch# configure terminal
Switch(config)# no ip pim rp-address 1.1.1.1
```

Related Commands

```
ip pim rp-candidate
ip pim rp-register-kat
```

8.4.16 ip pim rp-candidate

Command Purpose

Use this command to set the candidate rp.
To remove the candidate rp, use the no form of this command.

Command Syntax

```
ip pim rp-candidate IFNAME ( { priority PRIORITY | interval INTERVAL | group-list LIST } )
no ip pim rp-candidate ( IFNAME )
```

Parameter	Parameter Description	Parameter Value
IFNAME	The name of the interface to be the candidate rp	Support physical/aggregation/loopback/vlan/tunnel ports
PRIORITY	The Candidate-RP priority	0-255
INTERVAL	The C-RP advertisement interval in seconds	1-16383 seconds
LIST	Group ranges for this C-RP, only permit filters would be cared	Up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set the interface eth-0-1 to be the candidate rp:

```
Switch# configure terminal
Switch(config)# ip pim rp-candidate eth-0-1
This example shows how to cancel the configured candidate rp:
Switch# configure terminal
Switch(config)# no ip pim rp-candidate eth-0-1
```

Related Commands

```
ip pim rp-address
```

8.4.17 ip pim rp-register-kat

Command Purpose

Use this command to set the keepalive timer (KAT) for (S,G) at RP from PIM registers.

To reset this timer to default value, use the no form of this command.

Command Syntax

```
ip pim rp-register-kat TIME
no ip pim rp-register-kat
```

Parameter	Parameter Description	Parameter Value
TIME	The KAT time in seconds	1-65535 seconds

Command Mode

Global Configuration

Default

None

Usage

The register message send from dr will add an entry on rp. This entry will be aged when the keepalive timer expired which can be configured by this command.

Examples

This example shows how to set the keepalive timer to 100s at RP from PIM registers:

```
Switch# configure terminal
```

```
Switch(config)# ip pim rp-register-kat 100
```

This example shows how to reset this timer to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ip pim rp-register-kat
```

Related Commands

```
ip pim rp-address
ip pim rp-candidate
```

8.4.18 ip pim spt-switch-threshold infinity

Command Purpose

Use this command to set the spt switch threshold to infinity.
To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim spt-switch-threshold infinity ( group-list LIST | )
no ip pim spt-switch-threshold infinity ( group-list LIST | )
```

Parameter	Parameter Description	Parameter Value
LIST	Group address access list	Up to 40 characters

Command Mode

Global Configuration

Default

The DR will switch to spt immediately when received the first multicast packet by default.

Usage

None

Examples

This example shows how to set the spt switch threshold to infinity:

```
Switch# configure terminal
Switch(config)# ip pim spt-switch-threshold infinity
This example shows how to reset the spt-switch-threshold to default:
Switch# configure terminal
Switch(config)# no ip pim spt-switch-threshold infinity
```

Related Commands

show ip pim sparse-mode spt-threshold

8.4.19 ip pim cisco-register-checksum

Command Purpose

Use this command to calculate register checksum over whole packet (cisco compatibility).
To remove this setting, use the no form of this command.

Command Syntax

```
ip pim cisco-register-checksum ( group-list LIST | )
no ip pim cisco-register-checksum ( group-list LIST | )
```

Parameter	Parameter Description	Parameter Value
LIST	Group address access list	Strings up to 40 characters

Command Mode

Global Configuration

Default

The register checksum defined in RFC is used by default.

Usage

The register checksum defined in RFC is used by default,if group-list is configured, only packets that verified can be sent in CISCO way.

Examples

This example shows how to set to calculate register checksum over whole packet:

```
Switch# configure terminal
Switch(config)# ip pim cisco-register-checksum
This example shows how to remove this setting:
Switch# configure terminal
Switch(config)# no ip pim cisco-register-checksum
```

Related Commands

None

8.4.20 ip pim sparse-mode

Command Purpose

Use this command to enable pim sparse mode on the interface.
To disable pim sparse mode, use the no form of this command.

Command Syntax

```
ip pim sparse-mode ( passive | )
no ip pim sparse-mode ( passive | )
```

Parameter	Parameter Description	Parameter Value
passive	Pim passive mode (local members only)	-

Command Mode

Interface Configuration

Default

Disable

Usage

The pim hello message will not be sent out from the interface when the passive mode is configured.

Examples

This example shows how to enable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim sparse-mode
```

This example shows how to disable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config-if)# no ip pim sparse-mode
```

This example shows how to enable pim sparse mode passive on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim sparse-mode passive
```

Related Commands

None

8.4.21 ip pim dense-mode**Command Purpose**

Use this command to enable pim dense mode on the interface.
To disable pim dense mode, use the no form of this command.

Command Syntax

```
ip pim dense-mode ( passive | )
no ip pim dense -mode
```

Parameter	Parameter Description	Parameter Value
passive	Pim passive mode (local members only)	-

Command Mode

Interface Configuration

Default

Disable

Usage

Pim sparse-mode and dense-mode can not take effect on the same interface. The pim hello message will not be sent out from the interface when the passive mode is configured.

Examples

This example shows how to enable pim dense mode on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim dense-mode
```

This example shows how to disable pim dense mode on the interface:

```
Switch# configure terminal
Switch(config-if)# no ip pim dense-mode
```

This example shows how to enable pim dense mode passive on the interface:

```
Switch# configure terminal
Switch(config-if)# ip pim dense-mode passive
```

Related Commands

None

8.4.22 ip pim propagation-delay

Command Purpose

Use this command to set propagation delay on its LAN.
To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim propagation-delay timer  
no ip pim propagation-delay
```

Parameter	Parameter Description	Parameter Value
timer	Propagation delay value	100-5000 ms

Command Mode

Interface Configuration

Default

1000ms

Usage

If all routers on a LAN support the LAN Prune Delay option, then the PIM routers on that LAN will use the values received to adjust their J/P_Override_Interval on that interface and the interface is LAN Delay Enabled

Examples

This example shows how to set propagation delay:

```
Switch# configure terminal  
Switch(config-if)# ip pim propagation-delay 400
```

This example shows how to unset this setting:

```
Switch# configure terminal  
Switch(config-if)# no ip pim propagation-delay
```

Related Commands

None

8.4.23 ip pim state-refresh origination-interval

Command Purpose

Use this command to set the interval of originator sending state refresh messages.
To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim state-refresh origination-interval INTERVAL  
no ip pim state-refresh origination-interval
```

Parameter	Parameter Description	Parameter Value
INTERVAL	state-refresh origination-interval	1-100 seconds

Command Mode

Interface Configuration

Default

60s

Usage

State Refresh Messages are generated periodically by the PIM-DM router directly connected to a source. This command can control the interval of two messages

Examples

This example shows how to set state-refresh origination-interval:

```
Switch# configure terminal
Switch(config-if)# ip pim state-refresh origination-interval 50
```

This example shows how to unset this setting:

```
Switch# configure terminal
Switch(config-if)# no ip pim state-refresh origination-interval
```

Related Commands

None

8.4.24 ip pim unicast-bsm

Command Purpose

Use this command to enable sending and receiving of unicast BSM for backward compatibility. To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim unicast-bsm
no ip pim unicast-bsm
```

Command Mode

Interface Configuration

Default

Disable

Usage

Interface will send BSM message to the whole pim domain by default.

Examples

This example shows how to enable sending and receiving of unicast BSM for backward compatibility:

```
Switch# configure terminal
Switch(config-if)# ip pim unicast-bsm
```

This example shows how to cancel this setting:

```
Switch# configure terminal
Switch(config-if)# no ip pim unicast-bsm
```

Related Commands

None

8.4.25 ip pim ssm

Command Purpose

Use this command to enable pim-ssm and set ssm group range. To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim ssm ( default | range LIST )
no ip pim ssm
```

Parameter	Parameter Description	Parameter Value
default	Use 232.0.0.0/8 group range for SSM	-
LIST	ACL for group range to be used for SSM	Up to 40 characters

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable pim-ssm and set ssm group range to default:

```
Switch# configure terminal
```

```
Switch(config-if)# ip pim ssm default
```

This example shows how to cancel this setting:

```
Switch# configure terminal
```

```
Switch(config-if)# no ip pim ssm default
```

Related Commands

None

8.4.26 show ip pim sparse-mode bsr-router**Command Purpose**

Use this command to show the information of bootstrap router.

Command Syntax

```
show ip pim sparse-mode bsr-router
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of bootstrap router:

```
Switch# show ip pim sparse-mode bsr-router
```

```
PIMv2 bootstrap information
```

```
This system is the bootstrap router (BSR)
```

```
BSR address: 12.0.9.2
```

```
Uptime: 00:00:08, BSR Priority: 64, Hash mask length: 10
```

```
Next bootstrap message in 00:00:04
```

```
Role: Candidate BSR
```

```
State: Elected BSR
```

```
Candidate RP: 12.0.9.2(eth-0-9)
```

```
Advertisement interval 60 seconds
```

```
Next C-RP advertisement in 00:00:57
```

Related Commands

None

8.4.27 show ip pim sparse-mode interface**Command Purpose**

Use this command to show the information of pim interface.

Command Syntax

show ip pim sparse-mode interface (detail |)

Parameter	Parameter Description	Parameter Value
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of pim interface:
Switch# show ip pim sparse-mode interface detail

```
eth-0-9 (vif 0):
  Address 12.0.9.1, DR 12.0.9.2
  Hello period 30 seconds, Next Hello in 26 seconds
  Triggered Hello period 5 seconds
  Neighbors:
    12.0.9.2
```

Related Commands

None

8.4.28 show ip pim sparse-mode local-member

Command Purpose

Use this command to show the pim local membership information.

Command Syntax

show ip pim sparse-mode local-member (IFNAME |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim local membership information:
Switch# show ip pim sparse-mode local-members

PIM local membership information

eth-0-3:

(*, 229.1.1.1) : Include

eth-0-9:

(*, 228.1.1.1) : Include

Related Commands

None

8.4.29 show ip pim sparse-mode mroute

Command Purpose

Use this command to show the mroute information of pim sparse mode.

Command Syntax

show ip pim sparse-mode mroute (*SRC_ADDR* | *GRP_ADDR* |) (detail |)

Parameter	Parameter Description	Parameter Value
SRC_ADDR	Source address	IPv4 Address
GRP_ADDR	Group address	IPv4 Address
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim mroute information:

Switch# show ip pim sparse-mode mroute detail

IP Multicast Routing Table

(* , RP) Entries: 0

(* , G) Entries: 2

(S , G) Entries: 0

(S , G , rpt) Entries: 0

FCR Entries: 0

(* , 228.1.1.1) Uptime: 00:09:55

RP: 0.0.0.0, RPF nbr: None, RPF idx: None

Upstream:

State: NOT JOINED, SPT Switch: Enabled, JT: off

Downstream:

eth-0-9:

State: NO INFO, ET: off, PPT: off

Assert State: NO INFO, AT: off

Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on

Local Olist:

eth-0-9

(* , 229.1.1.1) Uptime: 00:04:22

RP: 12.0.9.2, RPF nbr: 12.0.9.2, RPF idx: eth-0-9

Upstream:

State: JOINED, SPT Switch: Enabled, JT Expiry: 40 secs

Macro state: Join Desired,

Downstream:

eth-0-3:

State: NO INFO, ET: off, PPT: off

Assert State: NO INFO, AT: off

Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
 Macro state: Could Assert, Assert Track
 Local Olist:
 eth-0-3

Related Commands

None

8.4.30 show ip pim sparse-mode neighbor

Command Purpose

Use this command to show the neighbor information of pim sparse mode.

Command Syntax

show ip pim sparse-mode neighbor ((IFNAME (address |)) | detail |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vla n/tunnel ports
address	Neighbor address	-
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the neighbor information of pim sparse mode:
 Switch# show ip pim sparse-mode neighbor

Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority/Mode
12.0.9.2	eth-0-9	00:18:18 /00:01:20 v2	1	DR

Related Commands

None

8.4.31 show ip pim sparse-mode rp mapping

Command Purpose

Use this command to show group to rp mappings.

Command Syntax

show ip pim sparse-mode rp mapping

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display group to rp mappings:

```
Switch# show ip pim sparse-mode rp mapping
```

```
PIM group-to-RP mappings
```

```
Group(s): 224.0.0.0/4
```

```
RP: 12.0.9.2
```

```
Info source: 12.0.9.2, via bootstrap, priority 192
```

```
Uptime: 00:22:56, expires: 00:01:34
```

Related Commands

None

8.4.32 show ip pim sparse-mode rp-hash**Command Purpose**

Use this command to show the information of rp to be chosen based on group selected.

Command Syntax

```
show ip pim sparse-mode rp-hash GRP_ADDR
```

Parameter	Parameter Description	Parameter Value
GRP_ADDR	Multicast group address	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of rp to be chosen based on group 224.0.0.10:

```
Switch# show ip pim sparse-mode rp-hash 224.0.0.10
```

```
RP: 12.0.9.2
```

```
Info source: 12.0.9.2, via bootstrap
```

Related Commands

None

8.4.33 show ip pim sparse-mode spt-threshold**Command Purpose**

Use this command to show the rpt to spt threshold of pim sparse mode.

Command Syntax

```
show ip pim sparse-mode spt-threshold
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the rpt to spt threshold of pim sparse mode:
Switch# show ip pim sparse-mode spt-threshold

PIM sparse-mode immediately switches over to SPT upon receiving the first traffic

Related Commands

None

8.4.34 show ip pim dense-mode interface**Command Purpose**

Use this command to show the interface information of pim sparse mode.

Command Syntax

show ip pim dense-mode interface (detail |)

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the interface information of pim dense mode:
Switch# show ip pim dense-mode interface

Address	Interface	VIFIndex	Ver/	Nbr	
			Mode	Count	
2.2.2.1	eth-0-2	0	v2/D	0	
3.3.3.1	eth-0-3	2	v2/D	0	

Related Commands

None

8.4.35 show ip pim dense-mode mroute**Command Purpose**

Use this command to show the mroute information of pim dense mode.

Command Syntax

show ip pim dense-mode mroute

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim mroute information:

```
Switch# show ip pim dense-mode mroute
```

```
PIM-DM Multicast Routing Table
(2.2.2.2, 225.1.2.3)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-3, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
(2.2.2.2, 225.1.2.4)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-3, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

Related Commands

None

8.4.36 show ip pim dense-mode neighbor

Command Purpose

Use this command to show the neighbor information of pim dense mode.

Command Syntax

```
show ip pim sparse-mode neighbor ( detail | )
```

Parameter	Parameter Description	Parameter Value
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the neighbor information of pim dense mode:

```
Switch# show ip pim dense-mode neighbor
```

```
Neighbor-Address Interface      Uptime/Expires    Ver
4.4.4.4      eth-0-9      03d19h16m/00:01:29 v2
3.3.3.2      agg3        03d19h17m/00:01:37 v2
```

Related Commands

None

8.4.37 show ip pim dense-mode nexthop**Command Purpose**

Use this command to show the nexthop information of pim dense mode.

Command Syntax

show ip pim sparse-mode nexthop

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the nexthop information of pim dense mode:
Switch# show ip pim dense-mode nexthop

Destination	Nexthop Num	Nexthop Addr	Nexthop Interface	Metric	Pref
1.1.1.2	0	-	-	-	-

Related Commands

None

8.4.38 show ip pim dense-mode interface**Command Purpose**

Use this command to show the interface information of pim sparse mode.

Command Syntax

show ip pim dense-mode interface (detail |)

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the interface information of pim dense mode:
Switch# show ip pim dense-mode interface

Address	Interface	VIFIndex	Ver/	Nbr	
			Mode	Count	

2.2.2.1	eth-0-2	0	v2/D	0
3.3.3.1	eth-0-3	2	v2/D	0

Related Commands

None

8.4.39 show ip pim dense-mode mroute

Command Purpose

Use this command to show the mroute information of pim dense mode.

Command Syntax

show ip pim dense-mode mroute

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim mroute information:

```
Switch# show ip pim dense-mode mroute
```

```
PIM-DM Multicast Routing Table
(2.2.2.2, 225.1.2.3)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-3, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
(2.2.2.2, 225.1.2.4)
  Source directly connected on eth-0-2
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-2
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-3, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

Related Commands

None

8.4.40 show ip pim sparse-mode nexthop-virtual-pair

Command Purpose

Use this command to show the pim nexthop virtual address mapping information.

Command Syntax

show ip pim sparse-mode nexthop-virtual-pair

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the pim nexthop virtual address mapping information:
Switch# show ip pim sparse-mode nexthop-virtual-pair

```
pim nexthop address    virtual address
10.1.1.2               20.1.1.2
```

Related Commands

None

8.4.41 ip pim nexthop-address

Command Purpose

Use this command to set the virtual address of the pim nexthop address.
To cancel this setting, use the no form of this command.

Command Syntax

```
ip pim nexthop-address NEXTHOP-ADDRESS virtual-address VIRTUAL-ADDRESS
no ip pim nexthop-address ( NEXTHOP-ADDRESS | )
```

Parameter	Parameter Description	Parameter Value
NEXTHOP-ADDRESS	nexthop address	IPv4 Address
VIRTUAL-ADDRESS	virtual address	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

When PIM use virtual address to connect neighbour, Use this command to the virtual address of the pim nexthop address.

Examples

This example shows how to set a nexthop address with virtual address:
Switch# configure terminal
Switch(config-if)# ip pim nexthop-address 10.1.1.2 virtual-address 20.1.1.2
This example shows how to unset this setting:
Switch# configure terminal
Switch(config-if)# no ip pim nexthop-address

Related Commands

None

8.5 MVR Commands

8.5.1 Mvr

Command Purpose

Use this command to enable MVR. To disable MVR, use the no form of this command.

Command Syntax

```
mvr
no mvr
```

Command Mode

Global Configuration

Default

Disable

Usage

Enable MVR in the Switch, must disable ip multicast-routing before enable MVR.

Examples

This example shows how to enable MVR:

```
Switch# configure terminal
Switch(config)# no ip multicast-routing
Switch(config)# mvr
```

Related Commands

```
show mvr
```

8.5.2 mvr vlan

Command Purpose

Use this command to specify the MVR source vlan. To remove this setting, use the no form of this command.

Command Syntax

```
mvr vlan vlan VLAN_ID
no mvr vlan
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

None

Usage

The related vlan interface should be created before the configuration of the MVR source vlan.

Examples

This example shows how to configure source vlan of MVR. configure vlan 2 as source vlan of MVR:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config)# interface vlan 2
```



```
Switch(config-if)# exit
Switch(config)# mvr vlan 2
```

Related Commands

interface vlan

8.5.3 mvr group**Command Purpose**

Use this command to configure global group for MVR. To remove this setting, use the no form of this command.

Command Syntax

```
mvr group IP_ADDR ( COUNT | )
no mvr group address ( COUNT | )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	Multicast group address	IPv4 Address
COUNT	Count of contiguous groups	1-64

Command Mode

Global Configuration

Default

None

Usage

This command is used to create or delete a global static group.

Examples

This example shows how to create global static group from 238.255.0.1 to 238.255.0.50:

```
Switch# configure terminal
Switch(config)# mvr group 238.255.0.1 50
```

Related Commands

None

8.5.4 mvr source-address**Command Purpose**

Use this command to create or delete mvr source address. To remove this setting, use the no form of this command.

Command Syntax

```
mvr source-address IP_ADDR
no mvr source-address
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	Source ip address	IPv4 Address

Command Mode

Global Configuration

Default

10.0.0.1

Usage

None

Examples

```
Create mvr source address:  
Switch# configure terminal  
Switch(config)# mvr source-address 192.168.11.1  
Resume mvr source address as default IP address:  
Switch# configure terminal  
Switch(config)# no mvr source-address
```

Related Commands

None

8.5.5 mvr type

Command Purpose

Use this command to configure a switch-port as source port or receiver port. To remove this setting, use the no form of this command.

Command Syntax

```
mvr type ( source | receiver vlan VLAN_ID )  
no mvr type ( receiver vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
source	MVR source port	-
receiver	MVR receiver port	-
VLAN_ID	MVR receiver vlan ID	1-4094

Command Mode

Interface Configuration

Default

None

Usage

Before configure the interface as source port or receiver port. make sure the source port belong to source vlan, and the receiver port must not belong to source vlan.

Examples

```
Configure the eth-0-1 as source port, and configure the eth-0-2 as receiver port of vlan 2:  
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# mvr type source  
Switch(config)# interface eth-0-2  
Switch(config-if)# mvr type receiver vlan 2
```

Related Commands

None

8.5.6 show mvr

Command Purpose

Use this command to show mvr information.

Command Syntax

```
show mvr
```

Command Mode

Privileged EXEC

Default

None

Usage

Show mvr information.

Examples

This example shows how to display MVR information:
Switch# show mvr

```
MVR Running: TRUE
MVR Multicast VLAN: 10
MVR Source-address: 1.1.1.1
MVR Max Multicast Groups: 512
MVR Hw Rt Limit: 511
MVR Current Multicast Groups: 0
```

Related Commands

None

8.5.7 show mvr interface**Command Purpose**

Use this command to show mvr interface information.

Command Syntax

show mvr interface

Command Mode

Privileged EXEC

Default

None

Usage

Show mvr interface information.

Examples

This example shows how to display MVR interface information:
Switch# show mvr interface

Port	Type	VLAN	Status
eth-0-2	source	10	ACTIVE
eth-0-1	receiver	11	ACTIVE

Related Commands

None

8.5.8 show mvr group**Command Purpose**

Use this command to show mvr group learned from receiver port.

Command Syntax

```
show mvr group vlan VLAN_ID ( GRP_ADDR | )
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	MVR receiver vlan ID	1-4094
GRP_ADDR	Multicast group address	IPv4 Address

Command Mode

Privileged EXEC

Default

None

Usage

Show mvr group information learned from receiver port

Examples

This example shows how to display mvr group learned from receiver port:

```
Switch# show mvr groups
```

VLAN	Interface	Group-Address	Uptime	Expires-time
11	eth-0-1	227.0.0.1	00:25:51	00:04:19

Related Commands

None

8.5.9 show mvr group static

Command Purpose

Use this command to show mvr global static groups.

Command Syntax

```
show mvr group static global
```

Command Mode

Privileged EXEC

Default

None

Usage

Show mvr static configured group information.

Examples

This example shows how to display mvr global static groups:

```
Switch# show mvr groups static global
```

MVR Static Global Group:

```
227.0.0.1
227.0.0.2
227.0.0.3
227.0.0.4
227.0.0.5
227.0.0.6
227.0.0.7
227.0.0.8
227.0.0.9
227.0.0.10
```

Related Commands

None

8.5.10 show resource mvr**Command Purpose**

Use this command to display the resource usage of MVR.

Command Syntax

show resource mvr

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the resource usage of MVR:

Switch# show resource mvr

MVR Resource	Used	Capability
MVR Entry	0	511
MVR Member	0	1022

Related Commands

None

Chapter 9 IPv6 Multicast Commands

9.1 IPv6 Multicast-Routing Commands

9.1.1 Ipv6 multicast-routing

Command Purpose

Use this command to enable ipv6 multicast routing.
To disable ipv6 multicast routing, use the no form of this command.

Command Syntax

ipv6 multicast-routing
no ipv6 multicast-routing

Command Mode

Global Configuration

Default

Enable

Usage

None

Examples

This example shows how to enable ipv6 multicast routing:

```
Switch# configure terminal  
Switch(config)# ipv6 multicast-routing
```

This example shows how to disable ipv6 multicast routing:

```
Switch# configure terminal  
Switch(config)# no ipv6 multicast-routing
```

Related Commands

None

9.1.2 ipv6 multicast route-limit

Command Purpose

Use this command to set the maximum number of the multicast routes.

To reset it to default value, use the no form of this command.

Command Syntax

ipv6 multicast route-limit *LIMIT* (*THRESHOLD* |)

no ipv6 multicast route-limit

Parameter	Parameter Description	Parameter Value
LIMIT	Max number of multicast route entries	1-2048
THRESHOLD	Threshold at which to generate warning message	1-2048

Command Mode

Global Configuration

Default

Default maximum number of the multicast routes should be 2048.

Default threshold should be same as the maximum number of multicast routes.

Usage

None

Examples

This example shows how to set the maximum number of the multicast routes to 512:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 multicast route-limit 512
```

This example shows how to reset the maximum number of the multicast routes to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 multicast route-limit
```

Related Commands

show ipv6 mroute route-limit

9.1.3 show ipv6 mroute

Command Purpose

Use this command to display the ipv6 multicast routing table information.

Command Syntax

```
show ipv6 mroute ( sparse | ) ( count | summary | )
```

```
show ipv6 mroute IPV6_ADDR ( sparse | ) ( count | summary | )
```

```
show ipv6 mroute route-limit
```

Parameter	Parameter Description	Parameter Value
sparse	Show sparse multicast routes	-
count	Show number of multicast route entries	-
summary	Show abbreviated multicast route information	-
IPV6_ADDR	Show specify source or group address multicast route	IPv6 address
route-limit	Show max route limit value	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast routing table:

```
Switch# show ipv6 mroute
```

```
IPv6 Multicast Routing Table
```

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
```

```
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface
```

```
2001:1::1234, ff0e::1234:5678
```

```
uptime 00:00:02, stat expires 00:03:28
```

```
Owner PIM-SMv6, Flags: TF
```

```
  Incoming interface: eth-0/1
```

```
  Outgoing interface list:
```

```
    Register
```


eth-0-2

This example shows how to display multicast routing table summary information:

```
Switch# 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

2001:1::1234, ff0e::1234:5678

00:01:04/00:02:26, PIM-SMv6, Flags: TF

Related Commands

ipv6 multicast route-limit

ipv6 mroute-rpf

9.1.4 show ipv6 mif

Command Purpose

Use this command to display the multicast interface information.

Command Syntax

```
show ipv6 mif ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast interface information:

```
Switch# show ipv6 mif
```

Interface	Mif	Owner	Uptime
	Idx	Module	
eth-0-1	0	PIM-SMv6	00:00:05
Register	1	PIM-SMv6	00:00:05

Related Commands

ipv6 pim sparse-mode

9.1.5 show ipv6 multicast groups count

Command Purpose

Use this command to display the multicast group count.

Command Syntax

```
show ipv6 multicast groups count
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display multicast group number:

```
Switch# show ipv6 multicast groups count
```

```
multicast group record count:  1
multicast source record count: 0
multicast total record count:  1
multicast max record count:    2048
```

Related Commands

None

9.1.6 show resource mcast6

Command Purpose

Use this command to display ipv6 multicast resource information.

Command Syntax

```
show resource mcast6
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display ipv6 multicast resource information:

```
Switch# show resource mcast6
```

MCAST

Resource	Used	Capability
Mcast Entry	0	224
Mcast Member	0	1792

Related Commands

None

9.1.7 clear ipv6 mroute

Command Purpose

Use this command to clear the ipv6 multicast routing table information.

Command Syntax

```
clear ipv6 mroute (* | GRP_IPV6_ADDR ( SRC_IPV6_ADDR ) | )
```

Parameter	Parameter Description	Parameter Value
GRP_IPV6_ADDR	Clear specify group address multicast route	IPv6 address
SRC_IPV6_ADDR	Clear specify source address multicast route	IPv6 address
*	Clear all multicast routes	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all ipv6 multicast routing table information:

```
Switch# clear ipv6 mroute *
```

Related Commands

```
show ipv6 mroute
```

9.2 MLD Commands

9.2.1 ipv6 mld access-group

Command Purpose

Use this command to apply an access-list to the mld interface.

To remove this setting, use the no form of this command.

Command Syntax

ipv6 mld access-group *LISTNAME*

no ipv6 mld access-group

Parameter	Parameter Description	Parameter Value
LISTNAME	The name of the ipv6 access-list to be applied. The format of access-list should be ipv6.	A string with 1-20 characters

Command Mode

Interface Configuration

Default

Access-group is not configured on any mld interface by default.

Usage

No matter the source ipv6 prefix or the destination ipv6 prefix in ACE should take effect respectively. If ACE's action is deny, then the packet will be ignored; Otherwise if it matches one whose action is permit, then it will be processed regularly.

Examples

This example shows how to apply the access-list acl1 to the interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld access-group acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld access-group
```

Related Commands

show ipv6 mld interface

9.2.2 ipv6 mld immediate-leave group-list

Command Purpose

Use this command to apply an access-list to configure which groups support immediately-leave per interface.

To remove this setting, use the no form of this command.

Command Syntax

ipv6 mld immediate-leave group-list *LISTNAME*

no ipv6 mld immediate-leave

Parameter	Parameter Description	Parameter Value
LISTNAME	The name of the ipv6 access-list to be applied. The format of access-list should be ipv6.	-

Command Mode

Interface Configuration

Default

Access-group is not configured on any mld interface by default.

Usage

No matter the source ipv6 prefix or the destination ipv6 prefix in ACE should be take effect respectively. If ACE' s action is denied, then the packet should be ignored; Otherwise if it matches one whose action is permit, then it should be processed regularly.

Examples

This example shows how to apply an access-list to configure which groups support immediately-leave on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld immediate-leave group-list acl1
```

This example shows how to remove the access-list acl1 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld immediate-leave group-list
```

Related Commands

show ipv6 mld interface

9.2.3 ipv6 mld last-member-query-count

Command Purpose

Use this command to set the value of last member query count.

To return it to default value, use the no form of this command.

Command Syntax

ipv6 mld last-member-query-count *COUNT*

no ipv6 mld last-member-query-count

Parameter	Parameter Description	Parameter Value
COUNT	The value of last member query count, range is 2 to 7	2-7

Command Mode

Interface Configuration

Default

2

Usage

None

Examples

This example shows how to set the value of last member query count to 5:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld last-member-query-count 5
```

This example shows how to return the value of last member query count to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld last-member-query-count
```

Related Commands

```
show ipv6 mld interface
ipv6 mld last-member-query-interval
```

9.2.4 ipv6 mld last-member-query-interval

Command Purpose

Use this command to set the value of last member query interval.

To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld last-member-query-interval *INTERVAL*

no ipv6 mld last-member-query-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	The last member query interval value(ms)	1000-25500

Command Mode

Interface Configuration

Default

1000

Usage

None

Examples

This example shows how to set the last member query interval value to 10000ms:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping last-member-query-interval 2000
```

This example shows how to reset the last member query interval value to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping last-member-query-interval
```

Related Commands

show ipv6 mld interface

ipv6 mld last-member-query-count

9.2.5 ipv6 mld limit

Command Purpose

Use this command to set the max num of groups allowed.

To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld limit *NUMBER* (except *LISTNAME* |)

no ipv6 mld limit

Parameter	Parameter Description	Parameter Value
NUMBER	The max num of groups, range is 1 to 4096	1-4096
LISTNAME	Groups not to be counted	A string with 1-20 characters

Command Mode

Global Configuration & Interface Configuration

Default

4096

Usage

Max number of groups is 4096 by default,in global configuration mode, use this command to set number of groups for all ports, in interface configuration mode, use this command to set number of groups for one ports

Examples

This example shows how to set the max num of groups allowed to 1000 globally:

```
Switch# configure terminal
Switch(config)# ipv6 mld limit 1000
```

This example shows how to reset the max num of groups to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 mld limit
```

Related Commands

show ipv6 mld interface

9.2.6 ipv6 mld mroute-proxy

Command Purpose

Use this command to set the mroute-proxy port on this interface.

To remove it, use the no form of this command.

Command Syntax

```
ipv6 mld mroute-proxy IFNAME
no ipv6 mld mroute-proxy IFNAME
```

Parameter	Parameter Description	Parameter Value
IFNAME	The interface name of the mroute-proxy port	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Interface Configuration

Default

None

Usage

This command is used to set the mroute-proxy port on the interface. Only one mroute-proxy port can be set on the interface. When set it again, the new setting will overwrite the old one.

Examples

This example shows how to set the mroute-proxy port to eth-0-1 on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1
```

This example shows how to remove the mroute-proxy port on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld mroute-proxy
```

Related Commands

ipv6 mld proxy-service

9.2.7 ipv6 mld proxy-service

Command Purpose

Use this command to enable mld mroute proxy service on the interface.

To disable it, use the no form of this command.

Command Syntax

```
ipv6 mld proxy-service
no ipv6 mld proxy-service
```

Command Mode

Interface Configuration

Default

None

Usage

This command is used with command `ipv6 mld mroute-proxy` and to set the upstream interface of the mld group.

Examples

This example shows how to enable mld mroute proxy service on this interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld proxy-service
```

This example shows how to disable mld mroute proxy service:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld proxy-service
```

Related Commands

`ipv6 mld mroute-proxy`

9.2.8 ipv6 mld querier-timeout

Command Purpose

Use this command to set the mld previous querier timeout value.

To reset it to default value, use the no form of this command.

Command Syntax

`ipv6 mld querier-timeout` *INTERVAL*

`no ipv6 mld querier-timeout`

Parameter	Parameter Description	Parameter Value
INTERVAL	The mld previous querier timeout value, range is 60 to 300s.	60-300

Command Mode

Interface Configuration

Default

255s

Usage

None

Examples

This example shows how to set the mld previous querier timeout value to 100 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld querier-timeout 100
```

This example shows how to reset the mld previous querier timeout value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld querier-timeout
```

Related Commands

ipv6 mld query-interval
ipv6 mld query-max-response-time

9.2.9 ipv6 mld query-interval

Command Purpose

Use this command to set the mld query interval.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld query-interval *INTERVAL*
no ipv6 mld query-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	The value of mld query interval, range is 2 to 18000s.	2-18000

Command Mode

Interface Configuration

Default

125s

Usage

None

Examples

This example shows how to set the mld query interval to 300 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld query-interval 300
```

This example shows how to return the mld query interval to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld query-interval
```

Related Commands

ipv6 mld querier-timeout
ipv6 mld query-max-response-time

9.2.10 ipv6 mld query-max-response-time

Command Purpose

Use this command to set the mld query max response time.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld query-max-response-time *INTERVAL*
no ipv6 query-max-response-time

Parameter	Parameter Description	Parameter Value
INTERVAL	The mld query max response time, range is 1 to 25s.	1-25

Command Mode

Interface Configuration

Default

10s

Usage

Query max response time must be less than mld query interval.

Examples

This example shows how to set the mld query max response time to 20 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld query-max-response-time 20
```

This example shows how to return the mld query max response time to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld query-max-response-time
```

Related Commands

ipv6 mld querier-timeout
ipv6 mld query-interval

9.2.11 ipv6 mld robustness-variable

Command Purpose

Use this command to set the mld querier robustness variable value.
To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld robustness-variable *VALUE*
no ipv6 robustness-variable

Parameter	Parameter Description	Parameter Value
VALUE	The mld querier robustness variable value, range is 2 to 7.	2-7

Command Mode

Interface Configuration

Default

2

Usage

None

Examples

This example shows how to set the mld querier robustness variable value to 6:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld robustness-variable 6
```

This example shows how to reset the mld querier robustness variable value to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld robustness-variable
```

Related Commands

show ipv6 mld interface

9.2.12 ipv6 mld version**Command Purpose**

Use this command to set the mld version on interface.

To return it to default value, use the no form of this command.

Command Syntax

ipv6 mld version *NUMBER*

no ipv6 version

Parameter	Parameter Description	Parameter Value
NUMBER	The mld version on the interface	1-2

Command Mode

Interface Configuration

Default

1

Usage

None

Examples

This example shows how to set the mld version 2 on the interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 mld version 2
```

This example shows how to return the mld version to default value:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ipv6 mld version
```

Related Commands

show ipv6 mld interface

9.2.13 ipv6 mld static-group

Command Purpose

Use this command to configure the static multicast group on interface.

To delete static group, use the no form of this command.

Command Syntax

ipv6 mld static-group *GRP_IPV6_ADDR* (source *SRC_IPV6_ADDR* |)

no ipv6 mld static-group *GRP_IPV6_ADDR* (source *SRC_IPV6_ADDR* |)

Parameter	Parameter Description	Parameter Value
GRP_IPV6_ADDR	The multicast group address	IPv6 address
SRC_IPV6_ADDR	The multicast source address	IPv6 address

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure the static mld group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 mld static-group ff0e::1234
Switch(config-if)# ipv6 mld static-group ff0e::1234 source 2001::2
```

This example shows how to delete static mld group on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 mld static-group ff02::1234
```

Related Commands

show ipv6 mld groups

9.2.14 ipv6 mld ssm-map enable

Command Purpose

Use this command to enable mld ssm mapping.

To disable ssm mapping, use the no form of this command.

Command Syntax

```
ipv6 mld ssm-map enable
no ipv6 mld ssm-map enable
```

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable mld ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld ssm-map enable
```

This example shows how to disable mld ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld ssm-map enable
```

Related Commands

None

9.2.15 ipv6 mld ssm-map static

Command Purpose

Use this command to set mld ssm mapping.

To cancel ssm mapping setting, use the no form of this command.

Command Syntax

```
ipv6 mld ssm-map static LISTNAME SRC_IPV6_ADDR
```

```
no ipv6 mld ssm-map static LISTNAME SRC_IPV6_ADDR
```

Parameter	Parameter Description	Parameter Value
LISTNAME	Specify multicast group address range access list	A string with 1-20 characters
SRC_IPV6_ADDR	Multicast source address	IPv6 address

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to set mld ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld ssm-map static ipacl 2001::2
```

This example shows how to unset mld ssm mapping:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld ssm-map static ipacl 2001::2
```

Related Commands

None

9.2.16 clear ipv6 mld

Command Purpose

Use this command to clear mld groups.

Command Syntax

```
clear ipv6 mld group ( * | IPV6_ADDR )
```

Parameter	Parameter Description	Parameter Value
*	All multicast group address	-
IPV6_ADDR	Specify multicast group address	IPv6 address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld group all:

```
Switch# clear ipv6 mld
```

```
Switch# clear ipv6 mld group *
```

This example shows how to clear mld specified group:

```
Switch# clear ipv6 mld group ff02::1234
```

Related Commands

```
show ipv6 mld groups
```

9.2.17 clear ipv6 mld interface

Command Purpose

Use this command to clear mld groups on specified interface.

Command Syntax

clear ipv6 mld (group *IPV6_ADDR* | interface) *IFNAME*

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	Specify multicast group address	IPv6 address
IFNAME	Interface name	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld group on specified interface:

```
Switch# clear ipv6 mld group interface eth-0-1
```

Related Commands

show ipv6 mld groups

9.2.18 show ipv6 mld groups

Command Purpose

Use this command to show the information about mld groups.

Command Syntax

show ipv6 mld groups *IPV6_ADDR* (detail |)

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	Specify multicast group address	IPv6 address
detail	Detailed Information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the detail information about mld groups:

```
Switch# show ipv6 mld groups detail
```

```
MLD Connected Group Membership Details for eth-0/2
```

```
Interface:      eth-0/2
```

```
Group:          ff0e::1234:5678
```

```
Uptime:         00:00:10
```

```
Group mode:     Exclude (Expires: 00:04:10)
```

```
Last reporter:  fe80::1111:1111:1111:1111:1111:1111:1111
```

```
Source list is empty
```

Related Commands

None

9.2.19 show ipv6 mld groups interface

Command Purpose

Use this command to show the information about mld groups on interface.

Command Syntax

```
show ipv6 mld groups IFNAME ( IPv6_ADDR | ) ( detail | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports
IPv6_ADDR	Specify multicast group address	IPv6 address
detail	Detailed Information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about mld groups on interface eth-0-1:

```
Switch# show ipv6 mld groups eth-0-1
```

MLD Connected Group Membership

Group Address	Interface	Expires
ff0e::1234:5678	eth-0-2	00:03:01

Related Commands

None

9.2.20 show ipv6 mld groups count**Command Purpose**

Use this command to show mld group number.

Command Syntax

```
show ipv6 mld groups ( IFNAME | ) count
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the mld group number on interface eth-0-1:

```
Switch# show ipv6 mld groups eth-0-1 count
```

```
Dynamic multicast groups count: 1
```

```
Static multicast groups count: 0
```

```
Total multicast groups count: 1
```

Related Commands

None

9.2.21 show ipv6 mld interface

Command Purpose

Use this command to show the information about mld on interface.

Command Syntax

```
show ipv6 mld interface ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
<i>IFNAME</i>	Interface name	Support physical/aggregation/loopback/vla n/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about mld on interface eth-0-1:

```
Switch# show ipv6 mld interface eth-0-1
```

```
Interface eth-0-1 (Index 1)
MLD Active, Querier, Version 1 (default)
Internet address is fe80::9c7c:7eff:fe94:8300
MLD interface has 0 group-record states
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 1000 milliseconds
Group Membership interval is 260 seconds
```

Related Commands

None

9.3 MLD Snooping Commands

9.3.1 ipv6 mld snooping

Command Purpose

Use this command to enable mld snooping.

To disable mld snooping, use the no form of this command.

Command Syntax

```
ipv6 mld snooping ( vlan VLAN_ID | )
```

```
no ipv6 mld snooping ( vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

Mld Snooping can be enabled globally and per vlan. By default, mld snooping should be disabled globally and per vlan.

Examples

This example shows how to enable mld snooping:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping
```

This example shows how to disable mld snooping:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping
```

This example shows how to enable mld snooping on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10
```

This example shows how to disable mld snooping on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10
```

Related Commands

show ipv6 mld snooping

9.3.2 ipv6 mld snooping fast-leave

Command Purpose

Use this command to enable mld snooping fast leave.

To disable it, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan *VLAN_ID* |) fast-leave

no ipv6 mld snooping (vlan *VLAN_ID* |) fast-leave

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

This command will override immediate-leave setting.

Examples

This example shows how to enable mld snooping fast-leave:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping fast-leave
```

This example shows how to disable mld snooping fast-leave:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping fast-leave
```

Related Commands

show ipv6 mld snooping global

9.3.3 ipv6 mld snooping last-member-query-interval

Command Purpose

Use this command to set the last member query interval of mld snooping.

To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan *VLAN_ID* |) last-member-query-interval *INTERVAL*

no ipv6 mld snooping (vlan *VLAN_ID* |) last-member-query-interval

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The last member query interval	1000-25500

Command Mode

Global Configuration

Default

1000ms

Usage

Mld last member query interval can be configured per vlan. The default is 1000ms and the range is 1000-25500ms.

Examples

This example shows how to set the last member query interval:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping last-member-query-interval 2000
```

This example shows how to reset the last member query interval to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping last-member-query-interval
```

Related Commands

```
show ipv6 mld snooping
```

```
show ipv6 mld snooping vlan
```

9.3.4 ipv6 mld snooping global source-address

Command Purpose

Use this command to set the global source address.

To reset it to default value, use the no form of this command.

Command Syntax

```
ipv6 mld snooping global source-address IPV6_ADDR
```

```
no ipv6 mld snooping global source-address
```

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	The IPv6 address of source address	IPv6 Address

Command Mode

Global Configuration

Default

The default IPv6 address is :: (All zero in 128 bits IPv6 address)

Usage

Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples

This example shows how to set the global source address to fe80::1:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping global source-address fe80::1
```

This example shows how to reset the global source address to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping global source-address
```

Related Commands

show ipv6 mld snooping querier

9.3.5 ipv6 mld snooping max-member-num

Command Purpose

Use this command to set the max allowed member number.
To reset it to default value, use the no form of this command.

Command Syntax

```
ipv6 mld snooping ( vlan VLAN_ID | ) max-member-num NUMBER
no ipv6 mld snooping ( vlan VLAN_ID | ) max-member-num
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
NUMBER	The max member number of mld snooping	1-4096

Command Mode

Global Configuration

Default

4096

Usage

None

Examples

This example shows how to set the max member number of mld snooping to 1024:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping max-member-num 1024
```

This example shows how to reset the max member number to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping max-member-num
```

Related Commands

show ipv6 mld snooping global

show ipv6 mld snooping vlan

9.3.6 ipv6 mld snooping query-interval

Command Purpose

Use this command to set the mld snooping query-interval.

To reset the query-interval to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan *VLAN_ID* |) query-interval *INTERVAL*

no ipv6 mld snooping (vlan *VLAN_ID* |) query-interval

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The query-interval of mld snooping (seconds), range is 2 to 18000	2-18000

Command Mode

Global Configuration

Default

125s

Usage

Query interval can't less than the mld snooping query max response time.

Examples

This example shows how to set the mld snooping query interval to 64s:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping query-interval 64
```

This example shows how to reset the query-interval to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping query-interval
```

Related Commands

```
show ipv6 mld snooping querier
show ipv6 mld snooping querier vlan
```

9.3.7 ipv6 mld snooping query-max-response-time

Command Purpose

Use this command to set the mld snooping query-interval.
To return the query-interval to default value, use the no form of this command.

Command Syntax

```
ipv6 mld snooping ( vlan VLAN_ID | ) query-max-response-time TIME
no ipv6 mld snooping ( vlan VLAN_ID | ) query-max-response-TIME
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
TIME	The query max response time (seconds)	1-25

Command Mode

Global Configuration

Default

10s

Usage

Query interval can't less than the mld snooping query max response time.

Examples

This example shows how to set the mld snooping query max response time to 15s:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping query-max-response-time 15
```

This example shows how to return the query max response time to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping query-max-response-time
```

Related Commands

```
show ipv6 mld snooping querier
show ipv6 mld snooping querier vlan
```

9.3.8 ipv6 mld snooping report-suppression

Command Purpose

Use this command to enable report suppression.

To disable report suppression, use the no form of this command.

Command Syntax

```
ipv6 mld snooping ( vlan VLAN_ID | ) report-suppression
```

```
no ipv6 mld snooping ( vlan VLAN_ID | ) report-suppression
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Enable

Usage

Will not do report suppression when MLD snooping works in v2 mode.

Examples

This example shows how to enable the report suppression:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping report-suppression
```

Related Commands

```
show ipv6 mld snooping
```

```
show ipv6 mld snooping vlan
```

9.3.9 ipv6 mld snooping version

Command Purpose

Use this command to set the mld snooping version.

To return it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan *VLAN_ID* |) version *VERSION*

no ipv6 mld snooping (vlan *VLAN_ID* |) version

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
VERSION	Mld snooping version, range is 1 to 2.	1-2

Command Mode

Global Configuration

Default

1

Usage

The default version is 1.

Examples

This example shows how to set the mld snooping version 2:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping version 2
```

Related Commands

show ipv6 mld snooping

show ipv6 mld snooping vlan

9.3.10 ipv6 mld snooping discard-unknown

Command Purpose

Use this command to enable discard unknown.

To disable discard unknown, use the no form of this command.

Command Syntax

ipv6 mld snooping (vlan *VLAN_ID* |) discard-unknown

no ipv6 mld snooping (vlan *VLAN_ID* |) discard-unknown

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Enabled by default, unknown multicast traffic will flood in vlan.

Usage

None

Examples

This example shows how to enable discard-unknown multicast traffic:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping discard-unknown
```

Related Commands

show ipv6 mld snooping

show ipv6 mld snooping vlan

9.3.11 ipv6 mld snooping querier tcn

Command Purpose

Use this command to set MLD snooping querier TCN related parameters. To reset it to default value, use the no form of this command.

Command Syntax

ipv6 mld snooping querier tcn (enable | query-count *COUNT* | query-interval *INTERVAL* | query-max-response-time *TIME*)

no ipv6 mld snooping querier tcn (enable | query-count | query-interval | query-max-response-time)

Parameter	Parameter Description	Parameter Value
enable	MLD querier TCN query enable	-
COUNT	MLD querier TCN query count, default is 2.	1-10
INTERVAL	MLD querier TCN query interval, default is 10s.	1-255 seconds
TIME	MLD querier TCN query max response time, default is 5s	1-9 seconds

Command Mode

Global Configuration

Default

This feature is enabled by default, default query count is 2, default query interval is 10s, maximum response time is 5s

Usage

None

Examples

This example shows how to use ipv6 mld snooping querier tc command:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping querier tc query-count 2
```

Related Commands

show ipv6 mld snooping querier

9.3.12 ipv6 mld snooping vlan access-group

Command Purpose

Use this command to set mld snooping access group on vlan.

Command Syntax

ipv6 mld snooping vlan *vlan_id* access-group *acl*

no ipv6 mld snooping vlan *vlan_id* access-group

Parameter	Parameter Description	Parameter Value
vlan_id	Vlan ID, range is 1 to 4094.	1-4094
acl	IPv6 Named Standard Access list.	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to use apply access-group on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 access-group acl
```

This example shows how to remove access-group from vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 access-group
```

Related Commands

show ipv6 mld snooping vlan

9.3.13 ipv6 mld snooping vlan mrouter interface

Command Purpose

Use this command to set mld snooping mrouter interface on vlan.

Command Syntax

ipv6 mld snooping vlan *VLAN_ID* mrouter interface *IFNAME*

no ipv6 mld snooping vlan *vlan_id* mrouter interface *IFNAME*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
IFNAME	Mrouter interface on this vlan	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Global Configuration

Default

None

Usage

The specified interface must have already joined the configured vlan.

Examples

This example shows how to set eth-0-1 as mrouter interface on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 mrouter interface eth-0-1
```

This example shows how to unset eth-0-1 as mrouter interface on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 mrouter interface eth-0-1
```

Related Commands

show ipv6 mld snooping vlan

9.3.14 ipv6 mld snooping vlan mrouter-aging-interval

Command Purpose

Use this command to set mld snooping mrouter interface aging interval on vlan.

Command Syntax

```
ipv6 mld snooping vlan VLAN_ID mrouter-aging-interval INTERVAL
```

```
no ipv6 mld snooping vlan VLAN_ID mrouter-aging-INTERVAL
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	Dynamic mrouter interface aging interval on this vlan(seconds)	1-65535

Command Mode

Global Configuration

Default

255s

Usage

None

Examples

This example shows how to set dynamic mrouter interface aging interval as 100 seconds on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 mrouter-aging-interval 100
```

This example shows how to reset dynamic mrouter interface aging interval as default on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 mrouter-aging-interval
```

Related Commands

show ipv6 mld snooping vlan

9.3.15 ipv6 mld snooping vlan querier

Command Purpose

Use this command to enable mld snooping querier on vlan.

Command Syntax

ipv6 mld snooping vlan *VLAN_ID* querier

no ipv6 mld snooping vlan *VLAN_ID* querier

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

This example shows how to enable querier on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 querier
```

This example shows how to disable querier on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 querier
```

Related Commands

show ipv6 mld snooping querier vlan

9.3.16 ipv6 mld snooping vlan querier address

Command Purpose

Use this command to set mld snooping querier address on vlan.

Command Syntax

ipv6 mld snooping vlan *VLAN_ID* querier address *IPV6_ADDR*

no ipv6 mld snooping vlan *VLAN_ID* querier address *IPV6_ADDR*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
IPV6_ADDR	The address of querier on this vlan	IPv6 Address

Command Mode

Global Configuration

Default

None

Usage

Will use global configured source-address if vlan is not configured, otherwise, use source-address config from vlan.

Examples

This example shows how to set querier address on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 querier address fe80::1
```

This example shows how to unset querier address on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 querier address
```

Related Commands

```
show ipv6 mld snooping querier vlan
```

9.3.17 ipv6 mld snooping vlan querier-timeout

Command Purpose

Use this command to set mld previous querier timeout interval on this vlan.To reset it to default, use the no form of this command.

Command Syntax

ipv6 mld snooping vlan *VLAN_ID* querier-timeout *INTERVAL*

no ipv6 mld snooping vlan *vlan_id* querier-timeout

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
INTERVAL	The mld previous querier timeout interval on this VLAN (seconds)	60-300

Command Mode

Global Configuration

Default

255s

Usage

None

Examples

This example shows how to set previous querier timeout interval as 100 seconds on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 querier address 2001::2
```

This example shows how to reset previous querier timeout interval on vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 querier-timeout
```

Related Commands

show ipv6 mld snooping querier vlan

9.3.18 ipv6 mld snooping vlan static-group

Command Purpose

Use this command to add static mld group on this vlan.To remove this setting, use the no form of this command.

Command Syntax

ipv6 mld snooping vlan *VLAN_ID* static-group *GRP_IPV6_ADDR* (source *SRC_IPV6_ADDR* |) interface *IFNAME*

no ipv6 mld snooping vlan *VLAN_ID* static-group *GRP_IPV6_ADDR* (source *SRC_IPV6_ADDR* |) interface *IFNAME*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
GRP_IPV6_ADDR	The address of group configured on the specified interface.	IPv6 Address
SRC_IPV6_ADDR	The address of source configured on the specified interface.	IPv6 Address
IFNAME	The interface configured as a member of specified group on this vlan	Support physical/aggregation ports

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to add group ff0e::1234 on interface eth-0-11 of vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 mld snooping vlan 10 querier-timeout 100
```

This example shows how to remove group ff0e::1234 from interface eth-0-11 of vlan 10:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 mld snooping vlan 10 static-group ff0e::1234 interface eth-0-11
```

Related Commands

```
show ipv6 mld snooping group
```

9.3.19 clear ipv6 mld snooping group**Command Purpose**

Use this command to clear all mld snooping groups.

Command Syntax

```
clear ipv6 mld snooping ( group * | )
```

Parameter	Parameter Description	Parameter Value
*	All multicast group address	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld snooping group all:

```
Switch# clear ipv6 mld snooping
```

Related Commands

None

9.3.20 clear ipv6 mld snooping vlan group

Command Purpose

Use this command to clear mld snooping groups on vlan.

Command Syntax

clear ipv6 mld snooping vlan *VLAN_ID*

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear mld snooping group on vlan 10:

```
Switch# clear ipv6 mld snooping vlan 10
```

Related Commands

None

9.3.21 show ipv6 mld snooping global

Command Purpose

Use this command to show the global configurations of mld snooping.

Command Syntax

```
show ipv6 mld snooping global
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the global configurations of mld snooping:

```
Switch# show ipv6 mld snooping global
```

Global Mld Snooping Configuration

```
-----  
Mld Snooping                               :Enabled  
Mld Snooping Fast-Leave                     :Disabled  
Mld Snooping Version                       :1  
Mld Snooping Max-Member-Number             :4096  
Mld Snooping Unknown Multicast Behavior    :Flood  
Mld Snooping Report-Suppression            :Enabled
```

Related Commands

None

9.3.22 show ipv6 mld snooping groups

Command Purpose

Use this command to show the mld snooping groups.

Command Syntax

```
show ipv6 mld snooping groups
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mld snooping groups:

```
Switch# show ipv6 mld snooping groups
```

VLAN	Interface	Group Address	Uptime	Expire-time
1	eth-0-3	ff0e:2111:1111:1111:1111:1234:5678	00:00:04	00:04:16

Related Commands

None

9.3.23 show ipv6 mld snooping groups vlan

Command Purpose

Use this command to show the mld snooping groups on vlan.

Command Syntax

show ipv6 mld snooping groups vlan *VLAN_ID* (*group_address* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094
group-address	The address of group	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mld snooping groups on vlan 1:

```
Switch# show ipv6 mld snooping groups vlan 1
```

MLD Snooping groups for vlan1

Interface: eth-0-3

Group: ff0e:2111:1111:1111:1111:1234:5678

Uptime: 00:00:42

Group mode: Exclude (Expires: 00:03:38)

Last reporter: fe80:1111:1111:1111:1111:1111:1111

Source list is empty

Related Commands

None

9.3.24 show ipv6 mld snooping groups count

Command Purpose

Use this command to show the mld snooping groups number.

Command Syntax

show ipv6 mld snooping groups (vlan *VLAN_ID* |) count

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mld snooping groups number on vlan 1:

```
Switch# show ipv6 mld snooping groups vlan 1 count
```

```
Dynamic multicast groups count: 1
```

```
Static multicast groups count: 0
```

```
Total multicast groups count: 1
```

Related Commands

None

9.3.25 show ipv6 mld snooping querier**Command Purpose**

Use this command to show the configurations of mld snooping querier information.

Command Syntax

```
show ipv6 mld snooping querier ( vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the configurations of mld snooping querier on vlan 1:

```
Switch# show ipv6 mld snooping querier vlan 1
```

Global Mld Snooping Querier Configuration

```
-----
Version                               :1
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)      :10
Query-Interval (sec)               :125
Global Source-Address              :::
TCN Query Count                    :2
TCN Query Interval (sec)           :10
Vlan 1:   MLD snooping querier status
```

```
-----
Elected querier is : ::
```

```
-----
Admin state                          :Disabled
Admin version                        :1
Operational state                    :Non-Querier
Querier operational address          :::
Querier configure address            :N/A
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)      :10
Query-Interval (sec)               :125
Querier-Timeout (sec)               :255
```

Related Commands

None

9.3.26 show ipv6 mld snooping mrouter

Command Purpose

Use this command to show the information of mld snooping mrouter port on vlan.

Command Syntax

show ipv6 mld snooping mrouter (vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of mld snooping mrouter port on vlan 1:

```
Switch# show ipv6 mld snooping mrouter  vlan 1
```

VLAN	Interface	Mode	Uptime	Expires-time
2	eth-0-1	static	-	-

Related Commands

None

9.3.27 show ipv6 mld snooping vlan

Command Purpose

Use this command to show the configurations of mld snooping on vlan.

Command Syntax

show ipv6 mld snooping (vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
<i>VLAN_ID</i>	Vlan ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the configurations of mld snooping on vlan 1:

```
Switch# show ipv6 mld snooping vlan 1
```

Global Mld Snooping Configuration

```
-----
Mld Snooping                               :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                       :1
Mld Snooping Max-Member-Number             :4096
Mld Snooping Unknown Multicast Behavior    :Flood
Mld Snooping Report-Suppression            :Enabled
Vlan 2
-----
Mld Snooping                               :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Report-Suppression            :Enabled
Mld Snooping Version                       :1
Mld Snooping Max-Member-Number             :4096
Mld Snooping Unknown Multicast Behavior    :Flood
Mld Snooping Group Access-list             :N/A
Mld Snooping Mrouter Port                  :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

Related Commands

None

9.3.28 show resource l2mcast

Command Purpose

Use this command to display the resource usage of L2 mcast.

Command Syntax

show resource l2mcast

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show resource l2mcast command:

```
Switch# show resource l2mcast
```

L2MCAST

Resource	Used	Capability
=====		
L2 Mcast Entry	1	1024
L2 Mcast Member	2	8192

Related Commands

None

9.4 PIMv6 Commands

9.4.1 ipv6 pim accept-register

Command Purpose

Use this command to apply an access-list to limit the ipv6 pim register message received by rp.
To remove this setting, use the no form of this command.

Command Syntax

ipv6 pim accept-register list *LISTNAME*

no ipv6 pim accept-register

Parameter	Parameter Description	Parameter Value
LISTNAME	The name of the access-list to be applied.	A string with 1-20 characters

Command Mode

Global Configuration

Default

None

Usage

This feature is used to prevent the unauthorized user registered to the switch.

When enable this feature, the system will send back a register stop message when the unauthorized register message is received.

Examples

This example shows how to apply the access-list acl1 to limit the ipv6 pim register message received by rp:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim accept-register list acl1
```

This example shows how to remove the limits:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim accept-register
```

Related Commands

None

9.4.2 ipv6 pim anycast-rp

Command Purpose

Use this command to set anycast rendezvous-point.

To remove the configurations, use the no form of this command.

Command Syntax

```
ipv6 pim anycast-rp ANYCAST_RP_ADDR ANYCAST_MEMBER_ADDR
```

```
no ipv6 pim anycast-rp ANYCAST_RP_ADDR ( ANYCAST_MEMBER_ADDR | )
```

Parameter	Parameter Description	Parameter Value
ANYCAST_RP_ADDR	Anycast rp address	IPv6 address
IPv6 address	IPv6 address	IPv6 address

Command Mode

Global Configuration

Default

None

Usage

Should configure every router in the network, and must configure same RP address.

Examples

This example shows how to set anycast rendezvous-point:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim anycast-rp 2001::2 2001::10
```

This example shows how to remove the member in anycast rendezvous-point:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim anycast-rp 2001::2 2001::10
```

Related Commands

None

9.4.3 ipv6 pim bsr-candidate

Command Purpose

Use this command to configure the candidate bootstrap router (candidate BSR).

To remove the configurations, use the no form of this command.

Command Syntax

```
ipv6 pim bsr-candidate IFNAME (HASH_MASK (PRIORITY) |)
```

```
no ipv6 pim bsr-candidate
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports
HASH_MASK	Hash mask length for RP selection	0-128
PRIORITY	Priority value for candidate bootstrap router	0-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to configure the candidate BSR:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim bsr-candidate eth-0/1
```

This example shows how to cancel the candidate BSR configured:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim bsr-candidate
```

Related Commands

ipv6 pim bsr-border

9.4.4 ipv6 pim bsr-border

Command Purpose

Use this command to configure the border of pim domain.

To remove the configurations of the border of pim domain, use the no form of this command.

Command Syntax

```
ipv6 pim bsr-border
```

```
no ipv6 pim bsr-border
```

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure the border of pim domain:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim bsr-border
```

This example shows how to remove the configurations of the border of pim domain:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim bsr-border
```

Related Commands

ipv6 pim bsr-candidate

9.4.5 ipv6 pim dr-priority

Command Purpose

Use this command to configure the DR priority.

To return it to default value, use the no form of this command.

Command Syntax

```
ipv6 pim dr-priority PRIORITY
no ipv6 pim dr-priority
```

Parameter	Parameter Description	Parameter Value
PRIORITY	The DR priority	0-4294967294

Command Mode

Interface Configuration

Default

1

Usage

When a hello message without DR priority is received, it will be regarded to have the max DR priority and to be elected as DR. When more than one router's hello messages do not have DR priority, the one which have the highest ipv6 address will be elected as DR.

Examples

This example shows how to set the pim router DR priority to 1000:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim dr-priority 1000
```

This example shows how to return the pim router DR priority to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim dr-priority
```

Related Commands

None

9.4.6 ipv6 pim exclude-genid

Command Purpose

Use this command to exclude generation id option from pim hello packets on this interface.
To return to the default setting, use the no form of this command.

Command Syntax

```
ipv6 pim exclude-genid
no ipv6 pim exclude-genid
```

Command Mode

Interface Configuration

Default

Disable

Usage

GenerationID is the ID of a PIM neighbour, it is carried in PIM hello message, the receiver device will record every received GenerationID in the hello packet and check if GenerationID has changed, if GenerationID changed, will consider neighbour state changed and restart state machine.

Examples

This example shows how to exclude generation id option from pim hello packets on this interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim exclude-genid
```

This example shows how to return the generation id option to the default setting:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim exclude-genid
```

Related Commands

None

9.4.7 ipv6 pim hello-interval

Command Purpose

Use this command to configure the interval for pim hello packets on this interface.

To reset to the default setting, use the no form of this command.

Command Syntax

ipv6 pim hello-interval *INTERVAL*

no ipv6 pim hello-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	The pim hello message interval (second)	1-65535

Command Mode

Interface Configuration

Default

30s

Usage

None

Examples

This example shows how to set the pim hello message interval to 100s:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim hello-interval 100
```

This example shows how to reset the pim hello message interval to default value:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim hello-interval
```

Related Commands

None

9.4.8 ipv6 pim ignore-rp-set-priority

Command Purpose

Use this command to ignore RP set priority value.

To not ignore the priority, use the no form of this command.

Command Syntax

```
ipv6 pim ignore-rp-set-priority
no ipv6 pim ignore-rp-set-priority
```

Command Mode

Global Configuration

Default

Not ignore RP set priority value.

Usage

None

Examples

This example shows how to ignore RP set priority value:

```
Switch# configure terminal
Switch(config)# ipv6 pim ignore-rp-set-priority
```

This example shows how to return the configurations to default value:

```
Switch# configure terminal
Switch(config)# no ipv6 pim ignore-rp-set-priority
```


Related Commands

None

9.4.9 ipv6 pim jp-timer

Command Purpose

Use this command to set the join/prune timer value.

To return the timer to default value, use the no form of this command.

Command Syntax

ipv6 pim jp-timer *SECOND*

no ipv6 pim jp-timer

Parameter	Parameter Description	Parameter Value
SECOND	The Join/Prune timer value (second)	1-65535

Command Mode

Global Configuration

Default

60s

Usage

None

Examples

This example shows how to set the join/prune timer value to 100s:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim jp-timer 100
```

This example shows how to return the join/prune timer value to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim jp-timer
```

Related Commands

None

9.4.10 ipv6 pim neighbor-filter

Command Purpose

Use this command to add an access-list to filter the neighbor.

To remove this filter, use the no form of this command.

Command Syntax

ipv6 pim neighbor-filter *LISTNAME*

no ipv6 pim neighbor-filter

Parameter	Parameter Description	Parameter Value
LISTNAME	The name of the access-list	A string with 1-20 characters

Command Mode

Interface Configuration

Default

None

Usage

Neighbours would send hello message to eachother to establish connections with other neighbour, you can use this command to filter which neighbour can be connected or not.

Examples

This example shows how to establish neighbors based on access-list acl1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim neighbor-filter acl1
```

This example shows how to cancel the filter:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim neighbor-filter
```

Related Commands

None

9.4.11 ipv6 pim register-rate-limit

Command Purpose

Use this command to set the rate limit for pim registers.

To return the rate limit to default value, use the no form of this command.

Command Syntax

ipv6 pim register-rate-limit *LIMIT*

no ipv6 pim register-rate-limit

Parameter	Parameter Description	Parameter Value
LIMIT	The rate limit for pim registers send from DR to RP	1-65535

Command Mode

Global Configuration

Default

By default, will not limit PIM register messages, if a limit is set, PIM register messages will be discard when pakcet reached by this limit.

Usage

There is no rate limit for pim registers by default.

When the rate limit is configured, the exceed pim register message will be dropped on the rp.

Examples

This example shows how to set the rate limit for pim registers to 100 per second:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim register-rate-limit 100
```

This example shows how to cancel the rate limit:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim register-rate-limit
```

Related Commands

ipv6 pim register-rp-reachability

ipv6 pim register-source

ipv6 pim register-suppression

9.4.12 ipv6 pim register-source

Command Purpose

Use this command to set the source address for pim register.

To return the source address for pim register to default value, use the no form of this command.

Command Syntax

ipv6 pim register-source *IFNAME*

no ipv6 pim register-source

Parameter	Parameter Description	Parameter Value
IFNAME	The name of the interface. Use the address of this interface to be the source address for pim register	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Global Configuration

Default

The source address for pim register is the interface ipv6 address of dr by default.

Usage

None

Examples

This example shows how to set the source address for pim register to the ipv6 address of interface eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim register-source eth-0-1
```

This example shows how to return the source address for pim register to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim register-source
```

Related Commands

ipv6 pim register-rate-limit

ipv6 pim register-rp-reachability

ipv6 pim register-suppression

9.4.13 ipv6 pim register-rp-reachability

Command Purpose

Use this command to enable rp reachability check for pim registers.

To disable this check, use the no form of this command.

Command Syntax

ipv6 pim register-rp-reachability
no ipv6 pim register-rp-reachability

Command Mode

Global Configuration

Default

Disable.

Usage

None

Examples

This example shows how to enable rp reachability check for pim registers:

```
Switch# configure terminal  
Switch(config)#ipv6 pim register-rp-reachability
```

This example shows how to disable rp reachability check for pim registers:

```
Switch# configure terminal  
Switch(config)#no ipv6 pim register-rp-reachability
```

Related Commands

ipv6 pim register-rate-limit
ipv6 pim register-source

9.4.14 ipv6 pim register-suppression

Command Purpose

Use this command to set the register suppression time.
To return this time to default value, use the no form of this command.

Command Syntax

ipv6 pim register-suppression *SECOND*
no ipv6 pim register-suppression

Parameter	Parameter Description	Parameter Value
SECOND	The register suppression time in seconds	11-65535

Command Mode

Global Configuration

Default

60s

Usage

None

Examples

This example shows how to set the register suppression time to 100s:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim register-suppression 100
```

This example shows how to return the register suppression time to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim register-suppression
```

Related Commands

ipv6 pim register-rate-limit

ipv6 pim register-rp-reachability

ipv6 pim register-source

9.4.15 ipv6 pim rp-address

Command Purpose

Use this command to set the ipv6 pim rp (rendezvous point) address.

To remove it, use the no form of this command.

Command Syntax

```
ipv6 pim rp-address IPV6_ADDR ( LISTNAME | override | )
```

```
no ipv6 pim rp-address IPV6_ADDR ( LISTNAME | )
```

Parameter	Parameter Description	Parameter Value
IPV6_ADDR	The rp address	IPv6 address
LISTNAME	The name of an access-list	A string with 1-20 characters
override	Overrides dynamically learned RP mappings	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set the pim rp address to 2001::2:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim rp-address 2001::2
```

This example shows how to remove the rp address 2001::2:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim rp-address 2001::2
```

Related Commands

ipv6 pim rp-candidate

ipv6 pim rp-register-kat

9.4.16 ipv6 pim rp-candidate

Command Purpose

Use this command to set the candidate rp.

To remove the candidate rp, use the no form of this command.

Command Syntax

```
ipv6 pim rp-candidate IFNAME ( { priority PRIORITY | interval INTERVAL | group-list LISTNAME } | )
```

```
no ipv6 pim rp-candidate ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	The name of the interface to be the candidate rp	Support physical/aggregation/loopback/vlan/tunnel ports
PRIORITY	The Candidate-RP priority	0-255
INTERVAL	The C-RP advertisement interval in seconds	1-16383
LISTNAME	Group ranges for this C-RP, only permit filters would be cared	A string with 1-20 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set the interface eth-0-1 to be the candidate rp:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim rp-candidate eth-0-1
```

This example shows how to cancel the configured candidate rp:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim rp-candidate eth-0-1
```

Related Commands

ipv6 pim rp-address

9.4.17 ipv6 pim rp-register-kat**Command Purpose**

Use this command to set the keepalive timer (KAT) for (S,G) at RP from PIM registers.

To return this timer to default value, use the no form of this command.

Command Syntax

```
ipv6 pim rp-register-kat SECOND
```

```
no ipv6 pim rp-register-kat
```

Parameter	Parameter Description	Parameter Value
SECOND	The KAT time in seconds	1-65535

Command Mode

Global Configuration

Default

185s

Usage

The register message send from dr will add an entry on rp. This entry will be aged when the keepalive timer expired which can be configured by this command.

Examples

This example shows how to set the keepalive timer to 100s at RP from PIM registers:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim rp-register-kat 100
```

This example shows how to return this timer to default value:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim rp-register-kat
```

Related Commands

ipv6 pim rp-address

ipv6 pim rp-candidate

9.4.18 ipv6 pim spt-switch-threshold infinity

Command Purpose

Use this command to set the spt switch threshold to infinity.

To cancel this setting, use the no form of this command.

Command Syntax

```
ipv6 pim spt-switch-threshold infinity ( group-list LISTNAME | )
```

```
no ipv6 pim spt-switch-threshold infinity ( group-list LISTNAME | )
```

Parameter	Parameter Description	Parameter Value
<i>LISTNAME</i>	Group address access list	A string with 1-20 characters

Command Mode

Global Configuration

Default

The DR will switch to spt immediately when received the first multicast packet by default.

Usage

None

Examples

This example shows how to set the spt switch threshold to infinity:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim spt-switch-threshold infinity
```

This example shows how to return the spt-switch-threshold to default:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim spt-switch-threshold infinity
```

Related Commands

```
show ipv6 pim sparse-mode spt-threshold
```

9.4.19 ipv6 pim cisco-register-checksum

Command Purpose

Use this command to calculate register checksum over whole packet (cisco compatibility).

To remove this setting, use the no form of this command.

Command Syntax

```
ipv6 pim cisco-register-checksum ( group-list LISTNAME | )
```

```
no ipv6 pim cisco-register-checksum ( group-list LISTNAME | )
```

Parameter	Parameter Description	Parameter Value
<i>LISTNAME</i>	Group address access list	A string with 1-20 characters

Command Mode

Global Configuration

Default

The register checksum defined in RFC is used by default.

Usage

The register checksum defined in RFC is used by default,if group-list is configured, only packets that verified can be sent in CISCO way.

Examples

This example shows how to set to calculate register checksum over whole packet:

```
Switch# configure terminal
```

```
Switch(config)# ipv6 pim cisco-register-checksum
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 pim cisco-register-checksum
```

Related Commands

None

9.4.20 ipv6 pim sparse-mode

Command Purpose

Use this command to enable pim sparse mode on the interface.

To disable pim sparse mode, use the no form of this command.

Command Syntax

ipv6 pim sparse-mode (passive |)

no ipv6 pim sparse-mode (passive |)

Parameter	Parameter Description	Parameter Value
passive	Pim passive mode (local members only)	-

Command Mode

Interface Configuration

Default

Disable

Usage

The pim hello message will not be sent out from the interface when the passive mode is configured.

Examples

This example shows how to enable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim sparse-mode
```

This example shows how to disable pim sparse mode on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim sparse-mode
```

This example shows how to enable pim sparse mode passive on the interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# ipv6 pim sparse-mode passive
```

Related Commands

None

9.4.21 ipv6 pim unicast-bsm

Command Purpose

Use this command to enable sending and receiving of unicast BSM for backward compatibility.

To cancel this setting, use the no form of this command.

Command Syntax

```
ipv6 pim unicast-bsm  
no ipv6 pim unicast-bsm
```

Command Mode

Interface Configuration

Default

Disable

Usage

Interface will send BSM message to the whole pim domain by default.

Examples

This example shows how to enable sending and receiving of unicast BSM for backward compatibility:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# ipv6 pim unicast-bsm
```

This example shows how to cancel this setting:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# no ipv6 pim unicast-bsm
```

Related Commands

None

9.4.22 ipv6 pim ssm

Command Purpose

Use this command to enable pim-ssm and set ssm group range.

To cancel this setting, use the no form of this command.

Command Syntax

ipv6 pim ssm (default | range *LISTNAME*)

no ipv6 pim ssm

Parameter	Parameter Description	Parameter Value
default	Use FF3x::/32 group range for SSM	-
LISTNAME	ACL for group range to be used for SSM	A string with 1-20 characters

Command Mode

Global Configuration

Default

Disable

Usage

Enable pim-ssm and set ssm group range.

Examples

This example shows how to enable pim-ssm and set ssm group range to default:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ipv6 pim ssm default
```

This example shows how to cancel this setting:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ipv6 pim ssm default
```

Related Commands

None

9.4.23 show ipv6 pim sparse-mode bsr-router

Command Purpose

Use this command to show the information of bootstrap router.

Command Syntax

```
show ipv6 pim sparse-mode bsr-router
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of bootstrap router:

```
Switch# show ipv6 pim sparse-mode bsr-router
```

PIM6v2 Bootstrap information

This system is the Bootstrap Router (BSR)

BSR address: 2001:2::1 (?)

Uptime: 00:00:08, BSR Priority: 64, Hash mask length: 126

Next bootstrap message in 00:00:52

Role: Candidate BSR

State: Elected BSR

Related Commands

None

9.4.24 show ipv6 pim sparse-mode interface

Command Purpose

Use this command to show the information of pim interface.

Command Syntax

show ipv6 pim sparse-mode interface (detail |)

Parameter	Parameter Description	Parameter Value
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of pim interface:

```
Switch# show ipv6 pim sparse-mode interface detail
```

```
eth-0-1 (vif 0):
```

```
Address fe80::9c7c:7eff:fe94:8300, DR fe80::9c7c:7eff:fe94:8300
```

```
Hello period 30 seconds, Next Hello in 3 seconds
```

```
Triggered Hello period 5 seconds
```

```
Secondary addresses:
```

```
2001::1
```

```
Neighbors:
```

Related Commands

None

9.4.25 show ipv6 pim sparse-mode local-member

Command Purpose

Use this command to show the pim local membership information.

Command Syntax

show ipv6 pim sparse-mode local-member (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim local membership information:

```
Switch# show ipv6 pim sparse-mode local-members
```

```
PIM Local membership information
```

```
eth-0-2:
```

```
*, ff0e::1234:5678
```

```
info: Include
```

Related Commands

None

9.4.26 show ipv6 pim sparse-mode mroute

Command Purpose

Use this command to show the mroute information of pim sparse mode.

Command Syntax

```
show ipv6 pim sparse-mode mroute ( SRC_IPV6_ADDR | GROUP_IPV6_ADDR | ) ( detail | )
```

Parameter	Parameter Description	Parameter Value
SRC_IPV6_ADDR	Source address	IPv6 address
GROUP_IPV6_ADDR	Group address	IPv6 address
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display pim mroute information:

```
Switch# show ipv6 pim sparse-mode mroute detail
```

```
IPv6 Multicast Routing Table
```

```
(* ,*,RP) Entries: 0
```

```
(* ,G) Entries: 1
```

```
(S,G) Entries: 0
```

```
(S,G,rpt) Entries: 0
```

```
FCR Entries: 0
```

```
*, ff0e::1234:5678
```

```
Type: (*,G)
```

```
Uptime: 00:01:49
```

```
RP: ::, RPF nbr: None, RPF idx: None
```

```
Upstream:
```

```
State: JOINED, SPT Switch: Enabled, JT: off
```

```
Macro state: Join Desired,
```

```
Downstream:
```

```
eth-0-2:
```

```
State: NO INFO, ET: off, PPT: off
```

```
Assert State: NO INFO, AT: off
```

```
Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
```

```
Macro state: Could Assert, Assert Track
```

```
Local Olist:
```

```
eth-0-2
```

Related Commands

None

9.4.27 show ipv6 pim sparse-mode neighbor

Command Purpose

Use this command to show the neighbor information of pim sparse mode.

Command Syntax

show ipv6 pim sparse-mode neighbor ((*IFNAME* (*IPv6_ADDR* |)) | detail |)

Parameter	Parameter Description	Parameter Value
<i>IFNAME</i>	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports
<i>IPv6_ADDR</i>	Neighbor address	IPv6 address
detail	Detailed interface information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the neighbor information of pim sparse mode:

```
Switch# show ipv6 pim sparse-mode neighbor
```

Neighbor Address	Interface	Uptime/Expires	DR Pri/Mode
fe80::9c7c:7eff:fe94:8300	eth-0-9	00:00:40/00:01:44	1 / DR

Related Commands

None

9.4.28 show ipv6 pim sparse-mode rp mapping

Command Purpose

Use this command to show group to rp mappings.

Command Syntax

show ipv6 pim sparse-mode rp mapping

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display group to rp mappings:

```
Switch# show ipv6 pim sparse-mode rp mapping
```

```
RP: 2001:1::1
```

```
Info source: 2001:1::1, via bootstrap
```

Related Commands

None

9.4.29 show ipv6 pim sparse-mode rp-hash

Command Purpose

Use this command to show the information of rp to be chosen based on group selected.

Command Syntax

show ipv6 pim sparse-mode rp-hash *GROUP_IPV6_ADDR*

Parameter	Parameter Description	Parameter Value
GROUP_IPV6_ADDR	Multicast group address	IPv6 address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information of rp to be chosen based on group ff02::1234:

```
Switch# show ipv6 pim sparse-mode rp-hash ff02::1234
```

```
RP: 2001::2
```

Related Commands

None

9.4.30 show ipv6 pim sparse-mode spt-threshold**Command Purpose**

Use this command to show the rpt to spt threshold of pim sparse mode.

Command Syntax

```
show ipv6 pim sparse-mode spt-threshold
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the rpt to spt threshold of pim sparse mode:

```
Switch# show ipv6 pim sparse-mode spt-threshold
```

IPv6 PIM sparse-mode immediately switches over to SPT upon receiving the first traffic

Related Commands

None

9.5 MVR6 Commands

9.5.1 mvr6

Command Purpose

Use this command to enable or disable MVR6. To disable mvr6, use the no form of this command.

Command Syntax

```
mvr6
```

```
no mvr6
```

Command Mode

Global Configuration

Default

Disable

Usage

Enable MVR6 in the Switch, must disable ipv6 multicast-routing before enable MVR6.

Examples

This example shows how to enable MVR6:

```
Switch# configure terminal
```

```
Switch(config)# no ipv6 multicast-routing
```

```
Switch(config)# mvr6
```

Related Commands

```
show mvr6
```

9.5.2 mvr6 vlan

Command Purpose

Use this command to specify the MVR6 source vlan.To remove this setting, use the no form of this command.

Command Syntax

mvr6 vlan *VLAN_ID*

no mvr6 vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

None

Usage

The related vlan interface should be created before the configuration of the MVR6 source vlan.

Examples

This example shows how to configure source vlan of MVR6. configure vlan 2 as source vlan of MVR6:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config)# interface vlan 2
Switch(config-if)# exit
Switch(config)# mvr6 vlan 2
```

Related Commands

interface vlan

9.5.3 mvr6 group

Command Purpose

Use this command to configure global group for MVR6.To remove this setting, use the no form of this command.

Command Syntax

mvr6 group *IPv6_ADDR* (*COUNT* |)

no mvr6 group address (*COUNT* |)

Parameter	Parameter Description	Parameter Value
<i>IPv6_ADDR</i>	Multicast group address	IPv6 Address
<i>COUNT</i>	Count of contiguous groups	1-64

Command Mode

Global Configuration

Default

None

Usage

This command is used to create or delete a global static group.

Examples

This example shows how to create global static group from ff0e::1 to ff0e::50:

```
Switch# configure terminal
```

```
Switch(config)# mvr6 group ff0e::1 50
```

Related Commands

None

9.5.4 mvr6 source-address

Command Purpose

Use this command to create mvr6 source address. To reset it to default value, use the no form of this command.

Command Syntax

mvr6 source-address *IPv6_ADDR*

no mvr6 source-address

Parameter	Parameter Description	Parameter Value
<i>IPv6_ADDR</i>	Source ipv6 address	IPv6 Address

Command Mode

Global Configuration

Default

fe80::1

Usage

None

Examples

This example shows how to create mvr6 source address:

```
Switch# configure terminal
```

```
Switch(config)# mvr6 source-address 2001::2
```

This example shows how to resume mvr6 source address as default IPv6 address:

```
Switch# configure terminal
```

```
Switch(config)# no mvr6 source-address
```

Related Commands

None

9.5.5 mvr6 type

Command Purpose

Use this command to configure a switch-port as source port or receiver port. To remove this setting, use the no form of this command.

Command Syntax

```
mvr6 type ( source | receiver vlan VLAN_ID )
```

```
no mvr6 type ( receiver vlan VLAN_ID | )
```

Parameter	Parameter Description	Parameter Value
source	MVR6 source port	-
receiver	MVR6 receiver port	-
VLAN_ID	MVR6 receiver vlan	1-4094

Command Mode

Interface Configuration

Default

None

Usage

Configure the interface as source port or receiver port. The source port must belong to source vlan, and the receiver port must not belong to source vlan.

Examples

This example shows how to configure the eth-0-1 as source port, and configure the eth-0-2 as receiver port of vlan 2:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# mvr6 type source
Switch(config)# interface eth-0-2
Switch(config-if)# mvr6 type receiver vlan 2
```

Related Commands

None

9.5.6 show mvr6

Command Purpose

Use this command to show mvr6 information.

Command Syntax

```
show mvr6
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mvr6 information:

```
Switch# show mvr6
```

```
MVR6 Running: TRUE
MVR6 Multicast VLAN: 2
MVR6 Source-address: fe80::1
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 3
```

Related Commands

None

9.5.7 show mvr6 interface

Command Purpose

Use this command to show mvr6 interface information.

Command Syntax

```
show mvr6 interface
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mrv6 interface information:

```
Switch# show mvr6 interface
```

Port	Type	VLAN	Status
eth-0-2	source	10	ACTIVE
eth-0-1	receiver	11	ACTIVE

Related Commands

None

9.5.8 show mvr6 group

Command Purpose

Use this command to show mvr6 group learned from receiver port.

Command Syntax

show mvr6 group vlan *VLAN_ID* (*IPv6_ADDR* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	MVR6 receiver VLAN	1-4094
IPv6_ADDR	Multicast group address	IPv6 Address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mvr6 group learned from receiver port:

```
Switch# show mvr6 groups
```

VLAN	Interface	Group Address	Uptime	Expire-time
1	eth-0-3	ff0e:2111:1111:1111:1111:1234:5678	00:00:11	00:04:10

Related Commands

None

9.5.9 show mvr6 group static

Command Purpose

Use this command to show mvr6 global static groups.

Command Syntax

```
show mvr6 group static global
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display mvr6 global static groups:

```
Switch# show mvr6 groups static global
```

```
MVR6 Static Global Group:
```

```
ff0e::1234
```

```
ff0e::1235
```

```
ff0e::1236
```

```
ff0e:2111:1111:1111:1111:1234:5678
```

Related Commands

None

9.5.10 show resource mvr6

Command Purpose

Use this command to display the resource usage of MVR6.

Command Syntax

show resource mvr6

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the resource usage of MVR6:

```
Switch# show resource mvr6
```

MVR

Resource

Used

Capability

MVR Entry

4

224

L2 Mcast Member

1

1792

Related Commands

None

Chapter 10 Traffic Management Commands

10.1 QOS Commands

10.1.1 table-map

Command Purpose

To create or modify a mutation map and enter the mutation configuration mode, use the mutation command. To remove a mutaiton map, use the no form of this command.

Command Syntax

table-map NAME

no table-map NAME

Parameter	Parameter Description	Parameter Value
NAME	Name assigned to the mutation map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Global Configuration

Default

None

Usage

You can define a mutation map for each class of qos to be used to set cos or set dscp.

Examples

```
Switch# configure terminal
Switch(config)# table-map dscp-table
```

Related Commands

set cos

set dscp

show table-map

10.1.2 map

Command Purpose

To map from one vlaue to another one in a muation map.

Command Syntax

map from *FROM_VALUE* [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*]
to *TO_VALUE*
no map from *FROM_VALUE* [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*] [*FROM_VALUE*]
[*FROM_VALUE*] to *TO_VALUE*

Parameter	Parameter Description	Parameter Value
FROM_VALUE	Source value	range 0-63
TO_VALUE	Destination value	range 0-63

Command Mode

Default

None

Usage

You can set the mapping value in a mutation table. Set 8 values at most by one command and can be set repeatedly.

Examples

```
Switch# configure terminal
Switch(config)# table-map dscp-table
Switch(config-tmap)# map from 0 1 2 3 4 5 6 7 to 1
```

Related Commands

None

10.1.3 default

Command Purpose

To set the default action for unmapping value in a mutation map.

Command Syntax

default { *VALUE* | copy | ignore }
no default { *VALUE* | copy | ignore }

Parameter	Parameter Description	Parameter Value
VALUE	Set tablemap default value	0-63
copy	Set the default behavior for value not found in the table map to copy	range 0-63
ignore	Set the default behavior for value not found in the table map to ignore	-

Command Mode

Default

copy

Usage

Each mutation table has only one default action.

When the default action is not copy,it will become copy when you set no command.

When the default action is copy,it will become ignore when you set no command.

Examples

```
Switch# configure terminal
Switch(config)# table-map dscp-table
Switch(config-tmap)# default 1
Switch(config-tmap)# default copy
Switch(config-tmap)# default ignore
```

Related Commands

None

10. 1. 4 class-map type qos

Command Purpose

To create or modify a class map and enter the class-map configuration mode, use the class-map command. To remove a class map, use the no form of this command.

Command Syntax

class-map type qos *NAME*

no class-map *NAME*

Parameter	Parameter Description	Parameter Value
NAME	Name assigned to the class map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores. The name class-default is reserved.

Command Mode

Global Configuration

Default

None

Usage

You can define a class map for each class of traffic to be used in QoS policies. If the packet matches any of the criteria configured for this class map with the match command, then this class map is applied to the packet. If no execution strategy is specified (match-any or match-all), then the default value of match-any is applied to the traffic class.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
```

Related Commands

```
class type qos
show class-map
```

10. 1. 5 match access-group

Command Purpose

Use this command to configure a match criterion by referencing an access list in a class-map. To remove the access-list from a class-map, use the no form of this command.

Command Syntax

```
match access-group NAME
no match access-group NAME
```

Parameter	Parameter Description	Parameter Value
NAME	access-list name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Class-map Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match access-group example
```

Related Commands

10. 1. 6 match cos

Command Purpose

To define the class of traffic using the class of service (CoS) value in class map, use the match cos command. To remove the match on the CoS value, use the no form of this command.

Command Syntax

match cos [inner] COS

no match cos [inner] COS

Parameter	Parameter Description	Parameter Value
COS	Specified CoS value	0-7

Command Mode

Class-map Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match cos 5
```

Related Commands

10. 1. 7 match dscp

Command Purpose

To identify specific differentiated services code point (DSCP) values as a match criterion, use the match dscp command. To remove specified DSCP values as a match criterion, use the no form of this command.

Command Syntax

match dscp DSCP_STR

no match dscp DSCP_STR

Parameter	Parameter Description	Parameter Value
DSCP_STR	Specified DSCP value	0-63

Command Mode

Class-map Configuration

Default

None

Usage

Match criteria can be PHB string

Examples

```
Switch# configure terminal
Switch(config)# class-map type qos cmap_qos
Switch(config-cmap-qos)# match dscp af11
```

Related Commands

10. 1. 8 class-map type traffic-class

Command Purpose

To create or modify a class map and enter the class-map configuration mode, use the class-map command. To remove a class map, use the no form of this command.

Command Syntax

```
class-map type traffic-class NAME
no class-map NAME
```

Parameter	Parameter Description	Parameter Value
NAME	Name assigned to the class map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores. The name class-default is reserved.

Command Mode

Global Configuration

Default

None

Usage

This type class-map is used to identify traffic flows with different traffic class.

Examples

```
Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc
```

Related Commands

class type traffic-class
show class-map

10. 1. 9 match traffic-class

Command Purpose

To configure a class map to use a specific QoS traffic-class value as a match criterion, use the match traffic-class command. To remove the specified protocol as match criteria, use the no form of this command.

Command Syntax

match traffic-class CLASS-ID
no match traffic-class CLASS-ID

Parameter	Parameter Description	Parameter Value
CLASS-ID	Specified traffic class value .	The valid values are from 1 to 7.

Command Mode

Class-map Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# class-map type traffic-class cmap_tc
Switch(config-cmap-tc)# match traffic-class 6
```

Related Commands

class-map

10. 1. 10 policy-map type qos

Command Purpose

Use this command to create a policy map. To remove the policy-map, use the no form of this command.

Command Syntax

policy-map type qos NAME
no policy-map NAME

Parameter	Parameter Description	Parameter Value
NAME	Name assigned to the policy map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Global Configuration

Default

None

Usage

The policy-map can be attached to multiple physical ports at ingress directions.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
```

Related Commands

```
service-policy type qos
show policy-map
```

10. 1. 11 class type qos**Command Purpose**

To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command

Command Syntax

```
class type qos NAME
no class NAME
```

Parameter	Parameter Description	Parameter Value
NAME	Reference to a class map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Policy-map Configuration

Default

None

Usage

Policy actions in the first class that matches the traffic type are performed.

By default, the class-default class is created under every policy map in the system. You cannot change this mapping.

You cannot remove the class-default. If you attempt to delete the class-default class, the switch returns an error message.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap)# class type qos cmap1
```

Related Commands

```
policy-map type qos
class-map type qos
```

10. 1. 12 class type qos class-default

Command Purpose

To add a reference to the system default class that does not match any traffic class, use the class class-default command. To remove the system default class from the policy map, use the no form of this command.

Command Syntax

```
class type qos class-default
no class class-default
```

Command Mode

Policy-map Configuration

Default

None

Usage

Traffic that fails to match any class is assigned to a default class of traffic called class-default. You cannot delete this class

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos class-default
```

Related Commands

```
policy-map type qos
```

10. 1. 13 set cos

Command Purpose

Use this command to remark packet CoS value.

Command Syntax

```
set cos { [ inner ] COS | cos table NAME | dscp table NAME }
no set cos [ [ inner ] COS | cos table NAME | dscp table NAME ]
```

Parameter	Parameter Description	Parameter Value
COS	CoS value	range 0-7
NAME	Reference to a mutation map	-

Command Mode

Config-pmap-c Configuration

Default

Disabled

Usage

There are four ways to set cos. Each way can only be reset by its no command while "no set cos" command can reset all ways. "no set cos COS" command do not care COS value.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set cos 3
```

Related Commands

None

10. 1. 14 set dscp

Command Purpose

Use this command to mark DSCP value.

Command Syntax

```
set dscp { DSCP | PHB_STR | default | dscp table NAME | cos table NAME }
no set dscp [ DSCP | PHB_STR | default | dscp table NAME | cos table NAME ]
```

Parameter	Parameter Description	Parameter Value
DSCP	DSCP value	range 0-63
PHB_STR	PHB name	af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 ef df cs1 cs2 cs3 cs4 cs5 cs6 cs7
default	default value (000000)	-
NAME	Reference to a mutation map	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Config-pmap-c Configuration

Default

Disabled

Usage

There are three ways to set dscp. Each way can only be reset by its no command while "no set dscp" command can reset all ways. "no set dscp DSCP" command do not care DSCP value.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set dscp cs3
```

Related Commands

None

10. 1. 15 set traffic-class

Command Purpose

Use this command to set traffic flow's class ID.

Command Syntax

```
set traffic-class CLASS-ID
no set traffic-class
```

Parameter	Parameter Description	Parameter Value
CLASS-ID	traffic class ID	range is 0-7

Command Mode

Config-pmap-c Configuration

Default

None

Usage

Traffic flow with different traffic class ID would be given varieties of treatments in ingress and egress. This command has higher priority with policer set traffic-class command.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set traffic-class 3
```

Related Commands

None

10. 1. 16 set color

Command Purpose

Use this command to set traffic flow's color.

Command Syntax

```
set color { red | yellow }
no set color
```

Parameter	Parameter Description	Parameter Value
red	red color	-
yellow	yellow color	-

Command Mode

Config-pmap-c Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# set color red
```

Related Commands

None

10. 1. 17 Policer

Command Purpose

Use this command to rate-limit traffic matching this traffic class for a specified interface. To cancel rate limit, use the no form of this command.

Command Syntax

```
policer { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] | drop } | exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } ] [ statistics ]
policer pps { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] | drop } | exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } ] [ statistics ]
no policer
```

Parameter	Parameter Description	Parameter Value
color-blind	Do not care input packet's color	-
color-aware	Care input packet's color	-
pps	PPS mode, default is BPS mode	-
CIR	CIR - Commit Information Rate.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.
CBS	CBS - Commit Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
EIR	EIR - Excess Information Rate. When eir is not set, use RFC 2697. When eir is set, use RFC 4115.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.

Parameter	Parameter Description	Parameter Value
EBS	EBS - Excess Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
conform	The action when the traffic not exceed C bucket. The default action is transmit	-
exceed	On single bucket mode, is the action when the traffic exceed C bucket. The default action is drop. On double bucket mode, is the action when the traffic exceed C bucket and not exceed E bucket, the default action is transmit	-
violate	On single bucket mode, not support this action. On double bucket mode, is the action when the traffic exceed E bucket, the default action is drop.	-
transmit	transmit the packet	-
drop	drop the packet	-
set-traffic-class CLASS-ID	set traffic-class for the packet	range 0-7
statistics	enable policer statistics	-

Command Mode

Config-pmap-c Configuration

Default

None

Usage

Policer and aggregate-policer can not be set together in the same policy map. This command has lower priority with set traffic-class command.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# policer color-blind cir 50000 cbs 40000 ebs 30000 conform-action transmit exceed-action drop statistics
```

Related Commands

```
show policy-map type qos statistics interface policer
show policy-map type qos statistics policer
```

10. 1. 18 qos aggregate-policer

Command Purpose

Use this command to create an aggregate policer instance. The aggregate policer can be shared by multiple classes of traffic. To remove the aggregate policer instance, use the no form of this command.

Command Syntax

```

qos aggregate-policer NAME { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] | drop } | exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } } [ statistics ]
qos aggregate-policer NAME pps { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] | drop } | exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } } [ statistics ]
no qos aggregate-policer NAME

```

Parameter	Parameter Description	Parameter Value
NAME	Specify an aggregate-policer name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.
color-blind	Do not care input packet' s color	-
color-aware	Care input packet' s color	-
pps	PPS mode, default is BPS mode	-
CIR	CIR - Commit Information Rate.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.
CBS	CBS - Commit Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
EIR	EIR - Excess Information Rate. When eir is not set, use RFC 2697. When eir is set, use RFC 4115.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.
EBS	EBS - Excess Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
conform	The action when the traffic not exceed C bucket. The default action is transmit	-
exceed	On single bucket mode, is the action when the traffic exceed C bucket. The default action is drop. On double bucket mode, is the action when the traffic exceed C bucket and not exceed E bucket, the default action is transmit	-
violate	On single bucekt mode, not support this action. On double bucket mode, is the action when the traffic exceed E bucket, the default action is drop.	-
transmit	transmit the packet	-
drop	drop the packet	-
set-traffic-class CLASS-ID	set traffic-class for the packet	range 0-7
statistics	enable policer statistics	-

Command Mode

Global Configuration

Default

None

Usage

All the flow who use aggreagte policer will share the same bandwitdh, it is different with policer.

Examples

```
Switch# configure terminal
Switch(config)# qos aggregate-policer example color-aware cir 1000 cbs 2000 eir 3000 ebs 4000 exceed drop statistics
```

Related Commands

```
aggregate-policer
show qos aggregate-policer
```

10. 1. 19 aggregate-policer

Command Purpose

Use this command to rate-limit the aggregate traffic matching this traffic class for all interfaces in the same slot. To cancel rate limit, use the no form of this command.

Command Syntax

```
aggregate-policer NAME
no aggregate-policer
```

Parameter	Parameter Description	Parameter Value
NAME	Aggregate policer name.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Config-pmap-c Configuration

Default

Disabled

Usage

Policer and aggregate-policer can not be set together in the same policy map. This command has lower priority with set traffic-class command.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type qos pmap_qos
Switch(config-pmap-qos)# class type qos cmap_qos
Switch(config-pmap-qos-c)# aggregate-policer transmit 1
```

Related Commands

```
qos aggregate-policer
show qos aggregate policer
```

10. 1. 20 policy-map type traffic-class

Command Purpose

Use this command to create a policy map. To remove the policy-map, use the no form of this command.

Command Syntax

policy-map traffic-class NAME

Parameter	Parameter Description	Parameter Value
NAME	Specify a policy-map name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Global Configuration

Default

Disabled

Usage

This command is used to create policy map to identify traffic flows with different traffic class.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
```

Related Commands

service-policy traffic-class

10. 1. 21 **class type traffic-class**

Command Purpose

To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command.

Command Syntax

class type traffic-class NAME
no class NAME

Parameter	Parameter Description	Parameter Value
NAME	Reference to a class map.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Policy-map Configuration

Default

None

Usage

Using this command, traffic classified by traffic-class can be specified varieties of properties, such as priority, bandwidth, etc.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
```

Related Commands

```
policy-map type traffic-class
class-map type traffic-class
```

10. 1. 22 class type traffic-class class-default

Command Purpose

To add a reference to an existing class map in a policy map and enter the class mode, use the class command. To remove a class from the policy map, use the no form of this command.

Command Syntax

```
class type traffic-class NAME
no class NAME
```

Command Mode

Policy-map Configuration

Default

None

Usage

Using this command, traffic classified by traffic-class can be specified varieties of properties, such as priority, bandwidth, etc.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
```

Related Commands

```
policy-map type traffic-class
```

10. 1. 23 priority level

Command Purpose

To assign a strict priority level to a traffic class in a policy map, use the priority level command. To remove the mapping, use the no form of this command.

Command Syntax

```
priority level LEVEL
no priority level
```

Parameter	Parameter Description	Parameter Value
LEVEL	Specifies the strict-priority level.	range 0-7

Command Mode

Config-pmap-c Configuration

Default

None

Usage

When the level is the same, queues will be scheduled on WDRR mode, otherwise will be scheduled on SP mode.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# priority level 5
```

Related Commands

show qos interface egress

10. 1. 24 bandwidth percentage**Command Purpose**

Use this command to allocate a percentage of the interface bandwidth to a queue. To remove configuration, use the no form of this command.

Command Syntax

```
bandwidth percentage PERCENTAGE
no bandwidth percentage
```

Parameter	Parameter Description	Parameter Value
PERCENTAGE	Specifies the percentage of bandwidth of the underlying link rate.	The range is 1-100.

Command Mode

Config-pmap-c Configuration

Default

None

Usage

Total percentage of all queues is 100. Unused bandwidth is allocated to default class.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# bandwidth percentage 20
```

Related Commands

show qos interface egress

10. 1. 25 queue-limit

Command Purpose

Use this command to specify queue buffer.

Command Syntax

queue-limit SIZE [ecn-threshold THRESHOLD]
no queue-limit

Parameter	Parameter Description	Parameter Value
SIZE	Queue buffer cell number, 288 bytes per cell	range 32-15360.
THRESHOLD	ECN threshold, 288 bytes per cell, range 32-15360. ECN threshold default value is queue size if no set.	range 32-15360.

Command Mode

Config-pmap-c Configuration

Default

64 buffer cells for control traffic;
256 buffer cells for non-drop traffic.

Usage

Queue-limit, queue-limit dynamic and random-detect are conflict.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit 200
```

Related Commands

show qos interface egress

10. 1. 26 queue-limit dynamic

Command Purpose

Use this command to specify dynamic buffer for queue.

Command Syntax

queue-limit dynamic LEVEL

Parameter	Parameter Description	Parameter Value
LEVEL	Queue level	range 0-10

Command Mode

Config-pmap-c Configuration

Default

10

Usage

Queue buffer can be caculated by the following expression:

$\text{threshold} = (f / (1 + f)) * \text{remainCnt}$ ($f = 1/128 \sim 8$).

f mapping:

level factor percent of remain buffer

0 1/128 ~0.8%

1 1/64 ~1.5%

2 1/32 ~3%

3 1/16 ~6%

4 1/8 ~11%

5 1/4 20%

6 1/2 ~33%

7 1 50%

8 2 ~66%

9 4 ~80%

10 8 ~89%

Queue-limit, queue-limit dynamic and random-detect are conflict.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# queue-limit dynamic 2
```

Related Commands

show qos interface egress

10. 1. 27 random-detect

Command Purpose

Use this command to configure random detect parameters.

Command Syntax

random-detect maximum-threshold MAX [minimum-threshold MIN] [ecn]
no random-detect

Parameter	Parameter Description	Parameter Value
MAX	maximum value in buffer cell, 288 bytes per cell	range 32-1023.
MIN	minimum value in buffer cell, 288 bytes per cell. MIN default value is MAX / 8 if no set.	range 32-1023
ecn	enable ecn	-

Command Mode

Config-pmap-c Configuration

Default

None

Usage

Queue-limit, queue-limit dynamic and random-detect are conflict.

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# random-detect maximum-threshold 200 ecn
```

Related Commands

show qos interface egress

10. 1. 28 shape rate**Command Purpose**

Use this command to configure shaping for a traffic class of a physical port in absolute value mode. To remove shaping, use the no form of this command.

Command Syntax

```
shape rate RATE
no shape rate
```

Parameter	Parameter Description	Parameter Value
RATE	The value for commit information rate	range 0 - 100,000,000.

Command Mode

Config-pmap-c Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# policy-map type traffic-class pmap_tc
Switch(config-pmap-tc)# class type traffic-class cmap_tc
Switch(config-pmap-tc-c)# shape rate 100000
```

Related Commands

show qos interface egress

10. 1. 29 service-policy type qos

Command Purpose

Use this command to apply a policy-map to an interface to affect the traffic classification rules. To remove the policy-map from the interface, use the no form of this command.

Command Syntax

```
service-policy type qos input NAME
no service-policy type qos input
```

Parameter	Parameter Description	Parameter Value
NAME	Policy-map name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type qos input pmap_qos
```

Related Commands

policy-map type qos

10. 1. 30 service-policy type traffic-class

Command Purpose

Use this command to apply a policy-map to an interface to affect the traffic queuing rules. To remove the policy-map from the interface, use the no form of this command.

Command Syntax

service-policy type traffic-class NAME
no service-policy type traffic-class

Parameter	Parameter Description	Parameter Value
NAME	Policy-map name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Interface Configuration
Configure-qos-global-view

Default

None

Usage

This command is used to apply queuing and priority-flow-control parameters on interface.

Examples

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# service-policy type traffic-class pmap_tc
```

Related Commands

policy-map type qos
class-map type traffic-class

10. 1. 31 qos policer

Command Purpose

Use this command to configure a port-policer for an interface matching all traffic transmitted or received in different direction. To cancel the rate limit, use the no form of this command.

Command Syntax

```
qos policer input { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] | drop } |
exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } ] [ statistics ]
qos policer input pps { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit [ set-traffic-class CLASS-ID ] |
drop } | exceed { transmit [ set-traffic-class CLASS-ID ] | drop } | violate { transmit [ set-traffic-class CLASS-ID ] | drop } ] [ statistics ]
qos policer output { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit | drop } | exceed { transmit | drop } |
violate { transmit | drop } ] [ statistics ]
qos policer output pps { color-blind | color-aware } cir CIR [ cbs CBS ] [ eir EBS ] [ ebs EBS ] [ conform { transmit | drop } | exceed { transmit |
drop } | violate { transmit | drop } ] [ statistics ]
no qos policer { input | output }
```

Parameter	Parameter Description	Parameter Value
color-blind	Do not care input packet's color	-
color-aware	Care input packet's color	-
pps	PPS mode, default is BPS mode	-

Parameter	Parameter Description	Parameter Value
CIR	CIR - Commit Information Rate.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.
CBS	CBS - Commit Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
EIR	EIR - Excess Information Rate. When eir is not set, use RFC 2697. When eir is set, use RFC 4115.	On BPS mode, the range is 0-100,000,000 kbps; On PPS mode, the range is 0-148,809,523 kbps.
EBS	EBS - Excess Burst Size.	On BPS mode, the range is 0-640,000 bytes, default value is 640000; On PPS mode, the range is 0-7,600 packets, default value is 4400.
conform	The action when the traffic not exceed C bucket. The default action is transmit	-
exceed	On single bucket mode, is the action when the traffic exceed C bucket. The default action is drop. On double bucket mode, is the action when the traffic exceed C bucket and not exceed E bucket, the default action is transmit	-
violate	On single bucket mode, not support this action. On double bucket mode, is the action when the traffic exceed E bucket, the default action is drop.	-
transmit	transmit the packet	-
drop	drop the packet	-
set-traffic-class CLASS-ID	set traffic-class for the packet	range 0-7
statistics	enable policer statistics	-

Command Mode

Interface Configuration

Default

None

Usage

This command is used to configure policing on port level.

Examples

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos policer input color-blind cir 50000 cbs 40000 ebs 30000 exceed drop statistics
```

Related Commands

show qos interface statistics policer

10. 1. 32 qos shape rate

Command Purpose

Use this command to configure shaping for a physical port in absolute value mode. To remove port shaping, use the no form of this command.

Command Syntax

qos shape rate pir PIR (ecn-percentage PERCENTAGE |)
no qos shape rate

Parameter	Parameter Description	Parameter Value
RATE	Shaping rate	range 0 - 100,000,0000.
PERCENTAGE	ECN percentage value	50%-100%

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# qos shape rate 1000
```

Related Commands

None

10. 1. 33 show table-map

Command Purpose

Use this command to show mutation table information.

Command Syntax

show table-map NAME

Parameter	Parameter Description	Parameter Value
NAME	Mutation map' s name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show table-map dscp-table
```

```
table-map dscp-table
map from 4 to 3
default copy
```

Related Commands

table-map

10. 1. 34 show class-map**Command Purpose**

Use this command to show class map information.

Command Syntax

```
show class-map [ NAME ]
```

Parameter	Parameter Description	Parameter Value
NAME	Class map's name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show class-map cos1
```

```
CLASS-MAP-NAME: cos1 (qos)
match cos 1
```

Related Commands

class-map type qos

10. 1. 35 show policy-map

Command Purpose

Use this command to show policy map information.

Command Syntax

show policy-map [NAME]

Parameter	Parameter Description	Parameter Value
NAME	Policy map's name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show policy-map q1

POLICY-MAP-NAME: q1 (qos)
State: attached

CLASS-MAP-NAME: cos0
match cos 0
set traffic-class : 7
statistics : enable
policer color-aware cir 10000000 cbs 640000 ebs 640000 statistics
```

Related Commands

policy-map type qos

10. 1. 36 show qos aggregate-policer

Command Purpose

Use this command to show aggregator-policer information.

Command Syntax

show qos aggregator-policer NAME

Parameter	Parameter Description	Parameter Value
NAME	aggregate policer name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show qos aggregate-policer example
```

```
Aggregate policer: test
  color blind
  CIR 1000 kbps, CBS 640000 bytes, EBS 640000 bytes
  drop violate packets
```

Related Commands

aggregate-policer

10. 1. 37 **show qos interface ingress****Command Purpose**

Use this command to show interface ingress information.

Command Syntax

```
show qos interface NAME ingress { cos-policy | inner-cos-policy | dscp-policy | acl-policy }
```

Parameter	Parameter Description	Parameter Value
NAME	interface name	Support physical/aggregation/vlan ports
cos-policy	show cos mapping information	-
inner-cos-policy	show inner cos mapping information	-
dscp-policy	show dscp mapping information	-
acl-policy	show acl mapping information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show qos interface eth-0-1 ingress cos-policy
```

CoS	TC	Color	Mark-Type	Mark-Value
0	0	green	-	-
1	1	green	-	-
2	2	green	-	-
3	3	green	-	-
4	4	green	-	-
5	5	green	-	-
6	6	green	-	-
7	7	green	-	-

Related Commands

```
service-policy type qos
service-policy type traffic-class
```

10. 1. 38 show qos interface egress

Command Purpose

Use this command to show interface egress information.

Command Syntax

```
show qos interface IFNAME egress
```

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show qos interface eth-0-1 egress
```

TC	Priority	Bandwidth	Shaping(kbps)	Drop-Mode	Queue-Limit(Max/Min)	ECN
0	0	Remaining	-	dynamic	level 0	-
1	1	-	-	dynamic	level 0	-
2	2	-	-	dynamic	level 0	-
3	3	-	-	dynamic	level 0	-
4	4	-	-	dynamic	level 0	-
5	5	-	-	dynamic	level 0	-
6	6	-	-	dynamic	level 0	-
7	7	-	-	tail-drop	64	-

Related Commands

service-policy type qos

10. 1. 39 show qos aggregate-policer statistics

Command Purpose

Use this command to show aggregator-policer's statistics information.

Command Syntax

show qos aggregator-policer NAME statistics

Parameter	Parameter Description	Parameter Value
NAME	aggregate policer name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show qos aggregate-policer example statistics

Aggregate policer: example

rfc2697 bps color-aware

CIR 1000000 kbps, CBS 640000 bytes, EBS 640000 bytes

Conform packets transmit

Exceed packets transmit

Violate packets drop

Statistics:

Type	Packets	Bytes	Action
Conform 0		0	Transmit
Exceed 0		0	Transmit
Violate 0		0	Drop
Total 0		0	-

Related Commands

service-policy type traffic-class

10. 1. 40 show policy-map type qos statistics interface ace

Command Purpose

Use this command to show the ace statistics of policy-map on interface.

Command Syntax

show policy-map type qos statistics interface NAME input ace (ace-based | class-based |) (class CMAP-NAME |)

Parameter	Parameter Description	Parameter Value
NAME	interface name	-
input	The statistics of input direction will be shown	-
ace-based	The statistics of matching ace will be shown	-
class-based	statistics of class-map will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	-

Command Mode

Privileged EXEC

Default

None

Usage

Using this command, the flow policer stats can be shown when class-based is specified and flow policer stats is enabled. The statistics of ace-based and class-based have results only when the statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics interface eth-0-1 input ace class-based
```

```
Interface: eth-0-1
```

```
Input service policy type qos: q1
```

```
Class name: cos0, operator: match-any(match 0 bytes 0)
```

```
Class name: cos1, operator: match-any(match 0 bytes 0)
```

```
Switch# show policy-map type qos statistics interface eth-0-1 input ace ace-based
```

```
Interface: eth-0-1
```

```
Input service policy type qos: q1
```

```
Class name: cos0, operator: match-any
match cos 0 ( 0 match 0 bytes)
```

```
total 0 match 0 bytes
```

```
Class name: cos1, operator: match-any
match cos 1 ( 0 match 0 bytes)
```

```
total 0 match 0 bytes
```

Related Commands

None

10. 1. 41 show policy-map type qos statistics vlan ace

Command Purpose

Use this command to show the ace statistics of policy-map on vlan.

Command Syntax

show policy-map type qos statistics vlan VLAN_ID input ace (ace-based | class-based |) (class CMAP-NAME |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN ID	1-4094
input	The statistics of input direction will be shown	-
ace-based	The statistics of matching ace will be shown	-
class-based	statistics of class-map will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

Using this command, the flow policer stats can be shown when class-based is specified and flow policer stats is enabled. The statistics of ace-based and class-based have results only when the statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics vlan 2 input ace class-based
```

```
Vlan: 2
Input service policy type qos: q1

Class name: cos0, operator: match-any(match 0 bytes 0)

Class name: cos1, operator: match-any(match 0 bytes 0)
```

```
Switch# show policy-map type qos statistics vlan 2 input ace ace-based
```

```
Vlan: 2
Input service policy type qos: q1

Class name: cos0, operator: match-any
match cos 0 ( 0 match 0 bytes)
total 0 match 0 bytes

Class name: cos1, operator: match-any
match cos 1 ( 0 match 0 bytes)
total 0 match 0 bytes
```

Related Commands

```
service-policy type qos
service-policy type traffic-class
```

10. 1. 42 show policy-map type qos statistics port-group ace

Command Purpose

Use this command to show the ace statistics of policy-map on port-group.

Command Syntax

show policy-map type qos statistics port-group *PG_NAME* input ace (ace-based | class-based |) (class *CMAP-NAME* |)

Parameter	Parameter Description	Parameter Value
PG_NAME	port-group name	Up to 32 characters
input	The statistics of input direction will be shown	-
ace-based	The statistics of matching ace will be shown	-
class-based	statistics of class-map will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

Using this command, the flow policer stats can be shown when class-based is specified and flow policer stats is enabled. The statistics of ace-based and class-based have results only when the statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics port-group pg input ace class-based
```

```
Port-group: pg
Input service policy type qos: q1

Class name: cos0, operator: match-any(match 0 bytes 0)

Class name: cos1, operator: match-any(match 0 bytes 0)
```

```
Switch# show policy-map type qos statistics vlan 2 input ace ace-based
```

```
Vlan: 2
Input service policy type qos: q1

Class name: cos0, operator: match-any
match cos 0 ( 0 match 0 bytes)
total 0 match 0 bytes
```

```
Class name: cos1, operator: match-any
match cos 1 ( 0 match 0 bytes)
total 0 match 0 bytes
```

Related Commands

```
service-policy type qos
service-policy type traffic-class
```

10. 1. 43 show policy-map type qos statistics vlan-group ace

Command Purpose

Use this command to show the ace statistics of policy-map on vlan-group.

Command Syntax

show policy-map type qos statistics vlan-group *VG_NAME* input ace (ace-based | class-based |) (class *CMAP-NAME* |)

Parameter	Parameter Description	Parameter Value
VG_NAME	vlan-group name	Up to 32 characters
input	The statistics of input direction will be shown	-

Parameter	Parameter Description	Parameter Value
ace-based	The statistics of matching ace will be shown	-
class-based	statistics of class-map will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

Using this command, the flow policer stats can be shown when class-based is specified and flow policer stats is enabled. The statistics of ace-based and class-based have results only when the statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics vlan-group vg input ace class-based
```

```
Vlan-group:  vg
Input service policy type qos: q1

Class name: cos0, operator: match-any(match 0 bytes 0)

Class name: cos1, operator: match-any(match 0 bytes 0)
```

```
Switch# show policy-map type qos statistics vlan 2 input ace ace-based
```

```
Vlan:  2
Input service policy type qos: q1

Class name: cos0, operator: match-any
match cos 0 ( 0 match 0 bytes)
total 0 match 0 bytes
```

```
Class name: cos1, operator: match-any
match cos 1 ( 0 match 0 bytes)
total 0 match 0 bytes
```

Related Commands

```
service-policy type qos
service-policy type traffic-class
```

10. 1. 44 show policy-map type qos statistics interface policer

Command Purpose

Use this command to show the policer statistics of policy-map on interface.

Command Syntax

```
show policy-map type qos statistics interface IFNAME input policer ( class CMAP-NAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Support physical/aggregation/vlan ports
input	The statistics of input direction will be shown	-

Parameter	Parameter Description	Parameter Value
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

The statistics have results only when the policer statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics interface eth-0-1 input policer
```

```
Interface: eth-0-1
```

```
Input service policy type qos: q1
```

```
Class name: cos0, operator : match-any
```

```
Class name: cos1, operator : match-any
```

```
Policer(mode rfc2697, rate mode bps, CIR 10000000 kbps, CBS 640000 bytes, EBS 640000 bytes, color mode color-aware, conform transmit, exceed transmit, violate drop)
```

```
Conform packets 0, bytes 0
```

```
Exceed packets 0, bytes 0
```

```
Violate packets 0, bytes 0
```

Related Commands

```
service-policy type qos
```

```
service-policy type traffic-class
```

10. 1. 45 show policy-map type qos statistics vlan policer

Command Purpose

Use this command to show the policer statistics of policy-map on vlan.

Command Syntax

```
show policy-map type qos statistics vlan VLAN_ID input policer ( class CMAP-NAME | )
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN ID	1-4094
input	The statistics of input direction will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

The statistics have results only when the policer statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics vlan 2 input policer
```

```
Vlan: 2
Input service policy type qos: q1

Class name: cos0, operator : match-any

Class name: cos1, operator : match-any
Policer(mode rfc2697, rate mode bps, CIR 10000000 kbps, CBS 640000 bytes, EBS 640000 bytes, color mode color-aware, conform
transmit, exceed transmit, violate drop)
Conform packets 0, bytes 0
Exceed packets 0, bytes 0
Violate packets 0, bytes 0
```

Related Commands

```
service-policy type qos
service-policy type traffic-class
```

10. 1. 46 show policy-map type qos statistics port-group policer**Command Purpose**

Use this command to show the policer statistics of policy-map on port-group.

Command Syntax

```
show policy-map type qos statistics port-group PG_NAME input policer ( class CMAP-NAME | )
```

Parameter	Parameter Description	Parameter Value
PG_NAME	port-group name	Up to 32 characters
input	The statistics of input direction will be shown	-
CMAP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

The statistics have results only when the policer statistics is enabled.

Examples

```
Switch# show policy-map type qos statistics port-group pg input policer
```

```
Port-group: pg
Input service policy type qos: q1

Class name: cos0, operator : match-any

Class name: cos1, operator : match-any
Policer(mode rfc2697, rate mode bps, CIR 10000000 kbps, CBS 640000 bytes, EBS 640000 bytes, color mode color-aware, conform
transmit, exceed transmit, violate drop)
```

Conform packets 0, bytes 0
Exceed packets 0, bytes 0
Violate packets 0, bytes 0

Related Commands

service-policy type qos
service-policy type traffic-class

10. 1. 47 show policy-map type qos statistics vlan-group policer

Command Purpose

Use this command to show the policer statistics of policy-map on vlan-group.

Command Syntax

show policy-map type qos statistics vlan-group *VG_NAME* input policer (class *CMP-NAME* |)

Parameter	Parameter Description	Parameter Value
VG_NAME	vlan-group name	Up to 32 characters
input	The statistics of input direction will be shown	-
CMP-NAME	statistics of the specified class-map can be shown	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

The statistics have results only when the policer statistics is enabled.

Examples

Switch# show policy-map type qos statistics vlan-group vg input policer

```
Vlan-group: vg
Input service policy type qos: q1

Class name: cos0, operator : match-any

Class name: cos1, operator : match-any
Policer(mode rfc2697, rate mode bps, CIR 10000000 kbps, CBS 640000 bytes, EBS 640000 bytes, color mode color-aware, conform
transmit, exceed transmit, violate drop)
Conform packets 0, bytes 0
Exceed packets 0, bytes 0
Violate packets 0, bytes 0
```

Related Commands

service-policy type qos
service-policy type traffic-class

10. 1. 48 show qos interface statistics policer

Command Purpose

Use this command to display port statistics.

Command Syntax

show qos interface IFNAME statistics policer (input | output)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

Switch# show qos interface eth-0-1 statistics policer input

```

Interface: eth-0-1
Input port policer:
  rfc2697    bps    color-aware
  CIR 2000000 kbps, CBS 640000 bytes, EBS 640000 bytes
  Conform packets transmit
  Exceed packets transmit
  Violate packets drop
Statistics:
  Type      Packets      Bytes      Action
  Conform 0          0          Transmit
  Exceed  0          0          Transmit
  Violate 0          0          Drop
Total    0          0          -

```

Related Commands

service-policy type qos

10. 1. 49 show qos interface statistics queue**Command Purpose**

Use this command to display the statistics of traffic class per interface.

Command Syntaxshow qos interface *IFNAME* statistics queue

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show qos interface eth-0/1 statistics queue
```

Queue	Transmit-packets	Transmit-Bytes	Drop-packets	Drop-Bytes
UC0	0	0	0	0
UC1	0	0	0	0
UC2	0	0	0	0
UC3	0	0	0	0
UC4	0	0	0	0
UC5	0	0	0	0
UC6	0	0	0	0
UC7	0	0	0	0
MC0	0	0	0	0
MC1	0	0	0	0
MC2	0	0	0	0
MC3	0	0	0	0
SPAN0	0	0	0	0

Related Commands

```
service-policy type traffic-class
```

10. 1. 50 clear qos aggregate-policer statistics**Command Purpose**

Use this command to clear aggregate policing statistics.

Command Syntax

```
clear qos aggregate-policer NAME statistics
```

Parameter	Parameter Description	Parameter Value
NAME	Aggregate policer name.	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear qos aggregate-policer example statistics
```

Related Commands

show qos aggregate-policer statistics

10. 1. 51 clear policy-map type qos statistics interface ace

Command Purpose

Use this command to clear the ace statistics of policy-map on interface.

Command Syntax

clear policy-map type qos statistics interface *IFNAME* input ace

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics interface eth-0-1 input ace
```

Related Commands

show policy-map type qos statistics interface ace

10. 1. 52 clear policy-map type qos statistics vlan ace

Command Purpose

Use this command to clear the ace statistics of policy-map on vlan.

Command Syntax

clear policy-map type qos statistics vlan *VLAN_ID* input ace

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics vlan 2 input ace
```

Related Commands

show policy-map type qos statistics vlan ace

10. 1. 53 **clear policy-map type qos statistics port-group ace**

Command Purpose

Use this command to clear the ace statistics of policy-map on port-group.

Command Syntax

```
clear policy-map type qos statistics port-group PG_NAME input ace
```

Parameter	Parameter Description	Parameter Value
PG_NAME	port-group name	Up to 32 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics port-group pg input ace
```

Related Commands

show policy-map type qos statistics port-group ace

10. 1. 54 clear policy-map type qos statistics vlan-group ace

Command Purpose

Use this command to clear the ace statistics of policy-map on vlan-group.

Command Syntax

clear policy-map type qos statistics vlan-group *VG_NAME* input ace

Parameter	Parameter Description	Parameter Value
<i>VG_NAME</i>	vlan-group name	Up to 32 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics vlan-group vg input ace
```

Related Commands

show policy-map type qos statistics vlan-group ace

10. 1. 55 clear policy-map type qos statistics ace

Command Purpose

Use this command to clear all the ace statistics of policy-map.

Command Syntax

show policy-map type qos statistics [input] ace

Parameter	Parameter Description	Parameter Value
input	The statistics of input direction will be clear	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics input ace
```

Related Commands

show policy-map type qos statistics ace

10. 1. 56 clear policy-map type qos statistics interface policer

Command Purpose

Use this command to clear the policer statistics of policy-map on interface.

Command Syntax

```
clear policy-map type qos statistics interface IFNAME input policer
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name.	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics interface eth-0-1 input policer
```

Related Commands

show policy-map type qos statistics interface policer

10. 1. 57 clear policy-map type qos statistics vlan policer

Command Purpose

Use this command to clear the policer statistics of policy-map on vlan.

Command Syntax

```
clear policy-map type qos statistics vlan VLAN_ID input policer
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics vlan 2 input policer
```

Related Commands

show policy-map type qos statistics vlan policer

10. 1. 58 clear policy-map type qos statistics port-group policer**Command Purpose**

Use this command to clear the policer statistics of policy-map on port-group.

Command Syntax

clear policy-map type qos statistics port-group *PG_NAME* input policer

Parameter	Parameter Description	Parameter Value
PG_NAME	port-group name	Up to 32 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics port-group pg input policer
```

Related Commands

show policy-map type qos statistics port-group policer

10. 1. 59 clear policy-map type qos statistics vlan-group policer**Command Purpose**

Use this command to clear the policer statistics of policy-map on vlan-group.

Command Syntax

clear policy-map type qos statistics vlan-group *VG_NAME* input policer

Parameter	Parameter Description	Parameter Value
VG_NAME	vlan-group name	Up to 32 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics vlan-group vg input policer
```

Related Commands

show policy-map type qos statistics vlan-group policer

10. 1. 60 clear policy-map type qos statistics policer**Command Purpose**

Use this command to clear all the policer statistics of policy-map.

Command Syntax

```
clear policy-map type qos statistics [ input ] policer
```

Parameter	Parameter Description	Parameter Value
input	The statistics of input direction will be clear	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear policy-map type qos statistics input policer
```

Related Commands

show policy-map type qos statistics policer

10. 1. 61 clear qos interface statistics policer**Command Purpose**

Use this command to clear port policer statistics.

Command Syntax

```
clear qos interface IFNAME statistics policer ( input | output )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name.	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear qos interface eth-0-1 statistics policer input
```

Related Commands

clear qos interface statistics policer

10. 1. 62 **clear qos vlan statistics policer**

Command Purpose

Use this command to clear vlan policer statistics.

Command Syntax

clear qos vlan *VLAN_ID* statistics policer (input | output)

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN_ID	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear qos vlan 2 statistics policer input
```

Related Commands

show qos vlan statistics policer

10. 1. 63 clear qos interface statistics queue

Command Purpose

Use this command to clear the queue statistics on specified interface.

Command Syntax

clear qos interface *IFNAME* statistics queue

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name.	Support physical/aggregation/vlan ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear qos interface eth-0-1 statistics queue
```

Related Commands

show qos interface statistics queue

10. 1. 64 flow-policer number

Command Purpose

To set the number of policers for qos, such as normal and extend mode.

Command Syntax

Flow-policer number (normal | extend)

Parameter	Parameter Description	Parameter Value
normal	Normal mode supports 576 policers	-
extend	Extend mode supports 3064 policers	-

Command Mode

Global Configuration

Default

Normal

Usage

When reset the number of policers, it needs to save the configuration and restart the switch.

Examples

```
Switch# configure terminal
Switch(config)# flow-policer number extend
```

% Configuration about flow-policer number has been stored, but cannot take effect until the next reload.

% When setting the extend number of policers, It only supports the 10G rate of policers, please check the rate of policers.

Related Commands

show policy-map type qos statistics interface ace

10. 1. 65 ipg shaping enable

Command Purpose

Use the ipg shaping enable to let shaping calculate IPG bytes. Use the no form of this command to return to the default setting.

Command Syntax

```
ipg shaping enable
no ipg shaping enable
```

Command Mode

Global Configuration

Default

Disabled

Usage

This command can be configured on global configure mode.

Examples

This example shows how to configure shaping to calculate IPG bytes:

```
Switch# configure terminal
```

```
Switch(config)# ipg shaping enable
```

This example shows how to disable shaping to calculate IPG bytes:

```
Switch# configure terminal
```

```
Switch(config)# no ipg shaping enable
```

Related Commands

None

10. 1. 66 **ipg policer enable**

Command Purpose

Uses the ipg policer enable to let policer calculate IPG bytes. Use the no form of this command to return to the default setting.

Command Syntax

ipg policer enable
no ipg policer enable

Command Mode

Global Configuration

Default

Disabled

Usage

This command can be configured on global configure mode and do not work on pps mode.

Examples

This example shows how to configure policer to calculate IPG bytes:

```
Switch# configure terminal
```

```
Switch(config)# ipg policer enable
```

This example shows how to disable policer to calculate IPG bytes:

```
Switch# configure terminal
```

```
Switch(config)# no ipg policer enable
```

Related Commands

None

10. 1. 67 **smart buffer enable**

Command Purpose

Use this command to enable queue drop smart buffer globally. Use the no form of this command to disable queue drop smart buffer globally.

Command Syntax

smart-buffer enable
no smart-buffer enable

Command Mode

Global Configuration

Default

Enable

Usage

This command can be configured on global configure mode.

Examples

This example shows how to enable the queue drop smart buffer.:

```
Switch# configure terminal
```

```
Switch(config)# smart-buffer enable
```

This example shows how to disable the queue drop smart buffer.:

```
Switch# configure terminal
```

```
Switch(config)# no smart-buffer enable
```

Related Commands

None

10. 1. 68 service-policy

Command Purpose

Use this command to apply a policy-map to member interfaces (member vlan) of the port group (vlan group) to affect the traffic classification rules. To remove the policy-map from the port group (vlan group), use the no form of this command.

Command Syntax

```
service-policy ( input | output ) NAME
```

```
no service-policy ( input | output )
```

Parameter	Parameter Description	Parameter Value
NAME	the policy-map name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.
input	apply policy-map to the inbound of member interfaces (member vlan)	-
output	apply policy-map to the outbound of member interfaces (member vlan)	-

Command Mode

Port-group Configuration

Vlan-group Configuration

Default

None

Usage

Use this command to apply a policy map defined by the policy-map command to the input or output of member interfaces (member vlan) of the port group (vlan group).

If the interface (vlan) has already been applied a policy-map, it cannot be added to the port group (vlan group).

Examples

Configure a policy to ingress of member interfaces of the port group :

```
Switch# configure terminal
```

```
Switch(config)# port-group port_group_1
```

```
Switch(config-port-group)# service-policy input plc_map1
```

Remove a policy from ingress of member interfaces of the port group :

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)# no service-policy input
```

Related Commands

policy-map

10. 1. 69 access-group

Command Purpose

Use this command to apply a policy-map to member interfaces (member vlan) of the port group (vlan group) to affect the traffic classification rules. To remove the policy-map from the port group (vlan group), use the no form of this command.

Command Syntax

```
access-group ( input | output ) NAME
no access-group ( input | output ) ( NAME | )
```

Parameter	Parameter Description	Parameter Value
NAME	the policy-map name	The name can be a maximum of 40 characters. The name is case sensitive and can only contain alphanumeric characters, hyphens, and underscores.
input	apply access-group to the inbound of member interfaces (member vlan)	-
output	apply access-group to the outbound of member interfaces (member vlan)	-

Command Mode

Port-group Configuration
Vlan-group Configuration

Default

None

Usage

Use this command to apply a access-group to the input or output of member interfaces (member vlan) of the port group (vlan group). If the interface (vlan) has already been applied a access-group, it cannot be added to the port group (vlan group).

Examples

Configure a access-group to ingress of member interfaces of the port group :

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)# access-group input access_group1
```

Remove a access-group from ingress of member interfaces of the port group :

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)# no access-group input
```

Related Commands

None

10. 1. 70 trust

Command Purpose

Use this command to configure the port trust state. To return to the default value, use the no form of this command.

Command Syntax

```
trust ( dscp | cos ( stag-cos | ctag-cos | ) | port )
no trust
```

Parameter	Parameter Description	Parameter Value
dscp	Trust DSCP indicates all incoming IP packets will be assigned with the priority and color according to the packet DSCP field, and for other packets, the priority and color of that packet will be mapped the same as trust CoS.	-
cos	Select which CoS will be specified for interface. The range of CoS is from 0 to 7.	-
ctag-cos	Trust ctag-cos indicates all incoming packets will be assigned with the priority and color according to the packet inner CoS field if the packet is double-tagged. If that packet is carried with only one VLAN tag or it is untagged, the behavior should be the same as that of trust port.	-
stag-cos	Trust stag-cos indicates all incoming packets will be assigned with the priority and color according to the packet outer CoS field if the packet is double-tagged. If that packet is carried with only one VLAN tag or it is untagged, the behavior should be the same as that of trust CoS.	-
port	Trust port indicates all incoming packets will be assigned with the priority and color according to the port CoS value.	-

Command Mode

Interface Configuration

Default

Trust the CoS value in packets.

Usage

The port trust state is the criteria for classifying incoming packets from the port. All classified packets will be identified with a priority and color according to the trust state. The default port trust state is trust cos.

Examples

This example shows how to configure the trust state:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# trust dscp
```

Related Commands

show qos interface

Chapter 11 Security Commands

11.1 Port Security Commands

11.1.1 clear port-security address-table static

Command Purpose

Use this command to clear static port-security mac address table.

Command Syntax

clear port-security address-table static (interface *IFNAME* | vlan *VLAN_ID* | address *MAC_ADDR* |)

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Clear port-security entries with specified mac address	MAC address in HHHH.HHHH.HHHH format
IFNAME	Clear port-security entries with specified interface name	Support physical/aggregation ports
VLAN_ID	Clear port-security entries with specified VLAN id	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all static port-security mac address-table:

```
Switch# clear port-security address-table static
```

This example shows how to clear static port-security mac address-table on eth-0-1:

```
Switch# clear port-security address-table static interface eth-0-1
```

Related Commands

show mac address-table

11.1.2 switchport port-security

Command Purpose

To enable port security on an interface, use the switchport port-security command. To disable port security, use the no switchport port-security command.

Command Syntax

```
switchport port-security  
no switchport port-security
```

Command Mode

Interface Configuration

Default

Disabled

Usage

When disable port-security, all the port-security mac address entries which are learnt dynamically will be cleared. The static port-security mac address will be ineffective but not be cleared.

Examples

This example shows how to enable port security on an interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport port-security
```

This example shows how to disable port security on an interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport port-security
```

Related Commands

show port-security interface

11.1.3 switchport port-security mac-address**Command Purpose**

Use this command to add static port-security mac address.

Command Syntax

```
switchport port-security mac-address MAC_ADDR vlan VLAN_ID
no switchport port-security mac-address MAC_ADDR vlan VLAN_ID
```

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Static port-security mac address	MAC address in HHHH.HHHH.HHHH format
VLAN_ID	Static port-security VLAN id	1-4094

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure static port-security mac address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport port-security mac-address 0.0.1 vlan 1
```

This example shows how to delete static port-security mac address:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport port-security mac-address 0.0.1 vlan 1
```

Related Commands

show mac address-table

11.1.4 switchport port-security maximum

Command Purpose

Use this command to set the maximum of secure MAC addresses on a port. Use the no switchport port-security maximum command to return to the default settings.

Command Syntax

switchport port-security maximum MAXIMUM
no switchport port-security maximum

Parameter	Parameter Description	Parameter Value
MAXIMUM	Maximum number of secure MAC addresses for the interface	0-16384

Command Mode

Interface Configuration

Default

1

Usage

If the new maximum is smaller than the current secure addresses on the interface, the configuration is rejected. Once the secure MAC address number on the port reached the maximum number, no more address can be learnt on that port. The maximum number 0 indicates that no dynamic secure MAC is allowed, only static secure MAC is supported.

Examples

This example sets the maximum number of secure MAC addresses on a port:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# switchport port-security maximum 1024
```

This example restores the maximum number of secure MAC addresses on a port to default value:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# no switchport port-security maximum
```

Related Commands

```
switchport port-security violation
```

```
show port-security maximum mac-num interface IFNAME
```

11.1.5 switchport port-security violation

Command Purpose

Use this command to set the action to be taken when a security violation is detected. Use the no switchport port-security violation command to return to the default settings.

Command Syntax

switchport port-security violation (protect | restrict | errdisable)
no switchport port-security violation

Parameter	Parameter Description	Parameter Value
protect	Discard packet silently	-
restrict	Discard packet and print log	-
errdisable	Discard packet, log and set the interface error-disabled	-

Command Mode

Interface Configuration

Default

Discard packet silently

Usage

To use this command, enable switchport port-security first

Examples

This example sets port-security violation to discard packets silently:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switch port-security violation protect
```

Related Commands

switchport port-security

11.1.6 show port-security address-table

Command Purpose

Use this command to show port-security mac address-table.

Command Syntax

show port-security address-table (static | dynamic |) (interface IFNAME | vlan VLAN_ID | address MAC_ADDR |)

Parameter	Parameter Description	Parameter Value
dynamic	Show the dynamically learnt entries	-
static	Show the statically configured entries	-
MAC_ADDR	Show the entries with specified mac address	MAC address in HHHH.HHHH.HHHH format
IFNAME	Show the entries with specified interface name	Support physical ports
VLAN_ID	Show the entries with specified VLAN id	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows port-security mac address-table on the Switch:

```
Switch# show port-security address-table
```

Secure Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0001.00ce.ef01	SecureConfigured	eth-0-11
41	001a.a02c.a1dc	SecureConfigured	eth-0-41

Related Commands

None

11.1.7 show port-security current mac-num interface

Command Purpose

Use this command to show current port-security MAC number on interface.

Command Syntax

show port-security current mac-num interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	Show the entries with specified interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows current port-security mac-num on interface eth-0-1:

```
Switch# show port-security current mac-num interface eth-0-1
```

```
Current dynamic MAC addresses : 0
```

```
Current static MAC addresses  : 0
```

```
Current total MAC addresses   : 0
```

Related Commands

switchport port-security maximum

show port-security maximum mac-num interface interface

11.1.8 show port-security interface

Command Purpose

Use this command to show the port-security information on an interface.

Command Syntax

show port-security interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	Show the entries with specified interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the port-security information on interface eth-0-1:

```
Switch# show port-security interface eth-0-1
```

```
Port Security          : disabled
Violation mode         : discard packet silence
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Static configured MAC Addresses : 1
```

Related Commands

None

11.1.9 show port-security maximum mac-num interface

Command Purpose

Use this command to show the port-security maximum MAC number on an interface.

Command Syntax

show port-security maximum mac-num interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	Show the entries with specified interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the port-security maximum mac-num on interface eth-0-1:

```
Switch# show port-security maximum mac-num interface eth-0-1
```

```
Maximum dynamic MAC addresses : 1
```

Related Commands

```
switchport port-security maximum
show port-security current mac-num interface
```

11.2 Vlan Security Commands

11.2.1 vlan mac-limit maximum

Command Purpose

Use this command to set maximum of mac addresses in specified vlan. Use the no vlan mac-limit maximum command to restore the default setting.

Command Syntax

```
vlan VLAN_ID mac-limit maximum MAXIMUM
no vlan VLAN_ID mac-limit maximum
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN id	1-4094
MAXIMUM	maximum of mac addresses	1-65535

Command Mode

VLAN Configuration

Default

No mac-limit on all vlans

Usage

The vlan must be created before this command

Examples

This example shows how to set/unset maximum of mac addresses for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# no vlan 2 mac-limit maximum
```

Related Commands

show vlan-security

11.2.2 vlan mac-limit action

Command Purpose

Use this command to set action for specified vlan.

Use the no vlan mac-limit action command to restore the default setting.

Command Syntax

vlan VLAN_ID mac-limit action (discard | warn | forward)

no vlan VLAN_ID mac-limit action

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN id	1-4094
discard	If the count of mac addresses reaches the maximum, packets with unknown source mac address from this VLAN will be discarded	-
warn	If the count of mac addresses reaches the maximum, packets with unknown source mac address from this VLAN will be discarded, and warning log will be printed in syslog	-
forward	If the count of mac addresses reaches the maximum, all packets from this VLAN will be forwarded without neither mac learning nor warning log	-

Command Mode

VLAN Configuration

Default

Forward

Usage

The vlan must be created before this command.

Examples

This example shows how to set/unset action for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch(config-vlan)# no vlan 2 mac-limit action
```

Related Commands

show vlan-security

11.2.3 vlan mac learning

Command Purpose

Use this command to enable/disable mac learning for specified vlan.

Command Syntax

vlan VLAN_ID mac learning (enable | disable)

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN id	1-4094
enable	Enable learning	-
disable	Disable learning	-

Command Mode

VLAN Configuration

Default

Enable

Usage

The vlan must be created before using this command.

Examples

This example shows how to enable mac learning for specified vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac learning enable
```

Related Commands

show vlan-security

11.2.4 show vlan-security

Command Purpose

Use this command to show configuration about vlan security.

Command Syntax

show vlan-security (vlan VLAN_ID)

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN id	1-4094

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show configuration about vlan security:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch# show vlan-security
```

Vlan	learning-en	max-mac-count	cur-mac-count	action
2	Enable	1000	0	Warn

Related Commands

vlan mac-limit maximum
 vlan mac-limit action

11.3 Time Range Commands

11.3.1 time-range

Command Purpose

Use this command to create time range and enter time-range configuration mode. Use the no time-range command to delete the time range.

Command Syntax

```
time-range TIME-RANGE-NAME
no time-range
```

Parameter	Parameter Description	Parameter Value
TIME-RANGE-NAME	The name of the time range	String with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

A time range is used to determine a range of time during which a filter is effective.

Examples

This example shows how to create a time range with the name "my-time-range":

```
Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)#
```

Related Commands

show time-range

11.3.2 absolute

Command Purpose

Use this command to define the absolute time and date in time range.

Command Syntax

```
absolute ( start HH:MM:SS MONTH DAY YEAR ) ( end HH:MM:SS MONTH DAY YEAR )
```

Parameter	Parameter Description	Parameter Value
start	Starting time and date	-
end	Ending time and date	-
HH:MM:SS	Starting time or Ending time	Hour,minute,second in HH:MM:SS format HH is 0-23
MONTH	Month	1-12
DAY	Day	1-31 (according to the month)
YEAR	Year	2000-2037

Command Mode

Time Range Configuration

Default

None

Usage

Comparing with the periodic time, choose an appropriate type.

Examples

This example shows how to define a time range started from 11:11:00 January 1 2008 and ended by 00:00:00 May 1 2009:

```
Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)# absolute start 11:11:00 jun 1 2008 end 00:00:00 may 1 2009
```

Related Commands

periodic

11.3.3 Periodic

Command Purpose

Use this command to define the periodic time and date in time range.

Command Syntax

periodic HH:MM WEEKDAY to HH:MM (WEEKDAY |)
periodic HH:MM (weekdays | weekend | daily) to HH:MM

Parameter	Parameter Description	Parameter Value
HH:MM	Starting time or Ending time	Hour,minute in HH:MM Format HH is 0-23
weekdays	Monday thru Friday	-
weekend	Saturday and Sunday	-
daily	Every day of the week	-
WEEKDAY	Day of the week(First three letters of the weekday)	A case insensitive string of Monday - Sunday, at least 3 characters when using abbreviation.

Command Mode

Time Range Configuration

Default

None

Usage

Comparing with the absolute time, choose an appropriate type.

Examples

This example shows how to define a time range started from 00:00 Monday and ended by 18:00 Wednesday in weekly period:

```
Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)# periodic 00:00 mon to 18:00 wed
This example shows how to define a time range started from 09:00 and ended by 17:00 every day:
Switch# configure terminal
Switch(config)# time-range my-time-range
Switch(config-tm-range)# periodic 09:00 daily to 17:00
```

Related Commands

Absolute

11.3.4 show time-range

Command Purpose

Use this command to show the information of time-range.

Command Syntax

show time-range (TIME-RANGE-NAME |)

Parameter	Parameter Description	Parameter Value
TIME-RANGE-NAME	the name of the time range. Show all the time ranges when the name is not specified	String with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

If no time range is specified, all time-ranges in the system should be shown.

Examples

This example shows how to display the information of all the time ranges:

```
Switch# show time-range

time-range range1
periodic 00:01 weekdays to 12:01
```

Related Commands

time-range

11. 4 ACL Commands

11.4.1 mac access-list

Command Purpose

Use this command to create MAC ACL and then enter MAC ACL in global configuration mode. Use no mac access-list command to delete the MAC ACL.

Command Syntax

```
mac access-list ACL_NAME
no mac access-list ACL_NAME
```

Parameter	Parameter Description	Parameter Value
ACL_NAME	The name of the MAC ACL	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has a MAC ACL with the same name, this command will enter the MAC ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.
When the name is not used by any ACL, this command is to create the MAC ACL firstly and then enter the MAC ACL configuration mode.

Examples

This example shows how to create a MAC ACL named list_mac_1 and then enter the MAC ACL configuration mode:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)#
```

This example shows how to remove the MAC ACL named list_mac_1:

```
Switch# configure terminal
Switch(config)# no mac access-list list_mac_1
```

Related Commands

match access-group

11.4.2 sequence-num

Command Purpose

Use this command to remove a filter from MAC ACL.

Command Syntax

no sequence-num SEQUENCE_NUM

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of a IP/MAC filter	1-131071

Command Mode

MAC ACL Configuration
IP ACL Configuration

Default

None

Usage

User can delete a ACL which is already attached to the class-map and used by a interface immediately.

Examples

This example shows how to remove a filter with the sequence-num 10 from MAC ACL:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# no sequence-num 10
```

This example shows how to remove a filter with the sequence-num 10 from IP ACL:

```
Switch# configure terminal
Switch(config)# ip access-list list_ip_1
Switch(config-ip-acl)# no sequence-num 10
```

Related Commands

```
deny
deny tcp
deny udp
deny icmp
deny igmp
permit
permit tcp
permit udp
permit icmp
permit igmp
```

11.4.3 deny src-mac

Command Purpose

Use this command to create a MAC filter for discarding ongoing packets matching the filter rule.

Command Syntax

```
( SEQUENCE_NUM | ) deny src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ) ( untag-vlan | ( ( vlan VLAN_ID ) ( cos COS ) ) ( inner-vlan INNER_VLAN ) ( inner-cos INNER_COS ) ) ( protocol ( arp ( arp-op-code ) | rarp | ETH_TYPE ) | packet-length OPERATOR LENGTH ) ( TIME_RANGE_NAME )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
any	Any host	-
MAC_ADDR MAC_ADDR_MASK	The MAC address and its wildcard bits	MAC and wildcard in HHHH.HHHH.HHHH format
host MAC_ADDR	The host with a specified MAC address	MAC address in HHHH.HHHH.HHHH format
dest-mac	Destination MAC address	-
untag-vlan	Without vlan tag	-
VLAN_ID	VLAN-ID	1-4094
COS	CoS Value	0-7
INNER_VLAN	Inner VLAN-ID	1-4094
INNER_COS	Inner CoS value	0-7
protocol	The protocol type which including ARP, RARP or Ether type	-
arp	ARP protocol	-
arp-op-code	arp-op-code	0-65535
rarp	RARP protocol	-
ETH_TYPE	Ether type	0-0xFFFF
TIME_RANGE_NAME	The time-range used by the MAC filter	A string with up to 40 characters

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

MAC ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110. Eth-type is not supported in egress ACL.

Examples

This example shows how to create a filter in MAC ACL to deny the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in MAC ACL to deny all the packets:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 2 deny src-mac any
```

This example shows how to create a filter in MAC ACL to deny the packet whose source MAC address is between the ranges specified:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

11.4.4 permit src-mac

Command Purpose

Use this command to create a MAC filter for allowing packets matching the filter rule to be delivered.

Command Syntax

```
( SEQUENCE_NUM | ) permit src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ) ( untag-vlan | ( vlan VLAN ) ) ( cos COS ) ( inner-vlan INNER_VLAN ) ( inner-cos INNER_COS ) ( protocol ( arp ( arp-op-code ) | rarp | ETH_TYPE ) | packet-length OPERATOR LENGTH ) ( TIME_RANGE_NAME )
```


Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
any	Any host	-
MAC_ADDR MAC_ADDR_MASK	The MAC address and its wildcard bits	MAC and wildcard in HHHH.HHHH.HHHH format
host MAC_ADDR	The host with a specified MAC address	MAC address in HHHH.HHHH.HHHH format
dest-mac	Destination MAC address	-
untag-vlan	Without vlan tag	-
VLAN	VLAN-ID	1-4094
COS	CoS	0-7
INNER_VLAN	Inner VLAN-ID	1-4094
INNER_COS	Inner CoS	0-7
protocol	The protocol type which including ARP, RARP or Ether type	-
arp	ARP protocol	-
arp-op-code	arp op code	0-65535
rarp	RARP protocol	-
ETH_TYPE	Ether type	0-0xFFFF
TIME_RANGE_NAME	Specify the name of time-range used by the MAC filter	String with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

MAC ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created MAC filter is 115. Eth-type is not supported in egress ACL.

Examples

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 1 permit src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in MAC ACL to permit all the packets:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 2 permit src-mac any
```

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address between the ranges specified:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

11.4.5 remark

Command Purpose

Use this command to add remarks for the MAC ACL.
To remove remarks of the MAC ACL, use the no form of this command.

Command Syntax

remark *REMARK*
no remark

Parameter	Parameter Description	Parameter Value
REMARK	The remarks of the MAC ACL	String with up to 100 characters

Command Mode

MAC ACL Configuration
IP ACL Configuration

Default

None

Usage

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples

This example shows how to add a remark to describe the MAC ACL:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# remark remark of List for mac
```

This example shows how to remove the remark of the MAC ACL:

```
Switch# configure terminal
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)# no remark
```

Related Commands

mac access-list

11.4.6 show access-list mac

Command Purpose

Use this command to show the MAC ACL information.

Command Syntax

show access-list mac (*ACL_NAME* |)

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	The name of the MAC ACL	String with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

If no mac acl are specified, all mac access-lists in the system should be shown.

Examples

This example shows how to show the MAC ACL information:

```
Switch# show access-list mac
```

```
mac access-list list_mac_1
 10 deny src-mac host 0000.0001.0002
 20 permit src-mac any
```

Related Commands

mac access-list

11.4.7 ip access-list

Command Purpose

Use this command to create IP ACL and then enter IP ACL configuration mode.
To remove this ACL, use the no form of this command.

Command Syntax

ip access-list *ACL_NAME*
no ip access-list *ACL_NAME*

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	The name of an IP ACL	String with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IP ACL with the same name, this command will enter the IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.
When the name is not used by any ACL, this command is to create the IP ACL firstly and then enter the IP ACL configuration mode.

Examples

This example shows how to create an IP ACL named list_ipv4_1 and then enter the IP ACL configuration mode:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)#
```

This example shows how to remove the IP ACL named list_ipv4_1:

```
Switch# configure terminal
Switch(config)# no ip access-list list_ipv4_1
```

Related Commands

match access-group

11.4.8 deny

Command Purpose

Use this command to discard ongoing IP packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny (*PROTO_NUM* | any) (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number	0-255
any	Any IP protocol	-
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-

Parameter	Parameter Description	Parameter Value
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

If IP address wildcard bit is provided, the IP address is logical-and in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created IP filter is 110.

Examples

This example shows how to create a filter in IP ACL to deny any IP packets:

This example shows how to create a filter in IP ACL to deny the fragment packets with the source IP addresss 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny any host 1.1.1.1 any fragments
```

This example shows how to create a filter in IP ACL to deny any routed packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 3 deny any any any routed-packet
```

Related Commands

no sequence-num

11.4.9 deny tcp

Command Purpose

Use this command to reject TCP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny tcp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC
DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established |
```

(match-any | match-all *FLAG-NAME* |) |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment)
 (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
established	Match established connections	-
match-any	Match any of the flag-name	-
FLAG-NAME	Match all the flag-name, including ack, fin, psh, rst, syn and urg	ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any TCP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny tcp any any
```

This example shows how to create a filter in IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in IP ACL to deny any TCP packets in established TCP streams:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 3 deny tcp any any established
```

This example shows how to create a filter in IP ACL to deny the TCP ACK packets with the source IP address 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

11.4.10 deny udp

Command Purpose

Use this command to reject UDP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny udp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC
DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment |
first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR
LENGTH | ) ( TIME_RANGE_NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address

Parameter	Parameter Description	Parameter Value
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.4.11 deny icmp

Command Purpose

Use this command to reject ICMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny icmp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment |
non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | )
( TIME_RANGE_NAME | )
```

Parameter	Parameter Description	Parameter Value
TYPE-NUM	ICMP message type	0-255
CODE-NUM	ICMP message code	0-255
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject ICMP packets.

Examples

This example shows how to create a filter in IP ACL to deny any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny icmp any any
```

This example shows how to create a filter in IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

11.4.12 deny igmp

Command Purpose

Use this command to reject IGMP packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny igmp (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (*IGMP-TYPE* |) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
IGMP-TYPE	IGMP type	including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-

Parameter	Parameter Description	Parameter Value
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject IGMP packets.

Examples

This example shows how to create a filter in IP ACL to deny any IGMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny igmp any any
```

This example shows how to create a filter in IP ACL to deny the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

11.4.13 deny gre

Command Purpose

Use this command to reject GRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM*) deny gre (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (*key KEY mask KEY-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP*) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet) (options) (packet-length *OPERATOR LENGTH*) (*TIME_RANGE_NAME*)

Parameter	Parameter Description	Parameter Value
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject GRE packets.
Please reference to command "deny" for the other parameters.

Examples

This example shows how to create a filter in IP ACL to deny any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny gre any any key 0 mask 0
```

This example shows how to create a filter in IP ACL to deny the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.4.14 deny nvgre

Command Purpose

Use this command to reject NVGRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny nvgre (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (vsid *VSID* mask *VSID-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)
Please reference to command "deny" for the other *parameters*.

Parameter	Parameter Description	Parameter Value
VSID	NVGRE vsid	0-16777215
VSID-MASK	NVGRE vsid mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number	0-255
any	Any IP protocol	-
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask

Parameter	Parameter Description	Parameter Value
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject NVGRE packets.

Examples

This example shows how to create a filter in IP ACL to deny any NVGRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 deny nvgre any any vsid 0 mask 0
```

This example shows how to create a filter in IP ACL to deny the NVGRE packets with the source IP address 1.1.1.1, any destination IP address and the nvgre vsid is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.4.15 permit

Command Purpose

Use this command to permit packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit (*PROTO_NUM* | any) (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number	0-255
any	Any IP protocol	-
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-

Parameter	Parameter Description	Parameter Value
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

If IP address wildcard bits are provided, the IP address is logical-and in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created IP filter is 115.

Examples

This example shows how to create a filter in IP ACL to permit any IP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 deny gre host 1.1.1.1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.4.16 permit tcp

Command Purpose

Use this command to permit TCP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit tcp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC
DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established |
( match-any | match-all FLAG-NAME | ) ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( TIME_RANGE_NAME | )
```


Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
established	Match established connections	-
match-any	Match any of the flag-name	-
FLAG-NAME	Match all the flag-name, including ack, fin, psh, rst, syn and urg	ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to permit any TCP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 10 permit any any any
```

This example shows how to create a filter in IP ACL to permit the TCP packets with the source IP address 1.1.1.1, and source port ranges from 0 to 100:

```
Switch# configure terminal
Switch(config-ex-ip-acl)# 20 permit tcp host 1.1.1.1 any non-first-fragments
```

This example shows how to create a filter in IP ACL to permit any TCP packets in established TCP streams:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 30 permit any any any routed-packet
```

This example shows how to create a filter in IP ACL to permit the TCP ACK packets with the source IP address 10.10.10.0:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

11.4.17 permit udp

Command Purpose

Use this command to permit UDP packets when the packets match this access-list.

Command Syntax

```
( SEQUENCE_NUM | ) permit udp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( src-port OPERATOR SRC_PORT | ) ( DST_MAC
DST_MAC_MASK | any | host DST_MAC ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment |
first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR
LENGTH | ) ( TIME_RANGE_NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filterin IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.4.18 permit icmp

Command Purpose

Use this command to permit ICMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit icmp ( SRC_MAC SRC_MAC_MASK | any | host SRC_MAC ) ( DST_MAC DST_MAC_MASK | any | host DST_MAC )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment |
non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | )
( TIME_RANGE_NAME | )
```

Parameter	Parameter Description	Parameter Value
icmp-type TYPE-NUM	ICMP message type	0-255
icmp-code CODE-NUM	ICMP message code	0-255

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit ICMP packets.

Examples

This example shows how to create a filter in IP ACL to permit any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit icmp any any
```

This example shows how to create a filter in IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

deny icmp
no sequence-num

11.4.19 permit igmp

Command Purpose

Use this command to permit IGMP packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit igmp (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (*IGMP-TYPE* |) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
IGMP-TYPE	IGMP type	IGMP type, including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7

Parameter	Parameter Description	Parameter Value
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit IGMP packets.

Examples

This example shows how to create a filter in IP ACL to permit any IGMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit igmp any any
```

This example shows how to create a filter in IP ACL to permit the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

11.4.20 permit gre

Command Purpose

Use this command to permit GRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit gre (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (key *KEY* mask *KEY-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)

Parameter	Parameter Description	Parameter Value
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit GRE packets.

Examples

This example shows how to create a filter in IP ACL to permit any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit gre any any key 0 mask 0
```

This example shows how to create a filter in IP ACL to permit the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.4.21 permit nvgre

Command Purpose

Use this command to permit NVGRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit nvgre (*SRC_MAC SRC_MAC_MASK* | any | host *SRC_MAC*) (*DST_MAC DST_MAC_MASK* | any | host *DST_MAC*) (vsid *VSID* mask *VSID-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (*TIME_RANGE_NAME* |)
Please reference to command "deny nvgre" for the other *parameters*.

Parameter	Parameter Description	Parameter Value
VSID	NVGRE vsid	0-16777215
VSID-MASK	NVGRE vsid mask	0-0xFFFFFFFF

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_MAC SRC_MAC_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_MAC	The source IP address of a host	IPv4 Address
DST_MAC DST_MAC_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_MAC	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit NVGRE packets.

Examples

This example shows how to create a filter in IP ACL to permit any NVGRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 1 permit nvgre any any vsid 0 mask 0
```

This example shows how to create a filter in IP ACL to permit the NVGRE packets with the source IP address 1.1.1.1, any destination IP address and the nvgre vsid is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)# 2 permit gre host 1.1.1.1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.4.22 show access-list ip

Command Purpose

Use this command to show the information of IP ACL.

Command Syntax

show access-list ip (ACL_NAME |)

Parameter	Parameter Description	Parameter Value
ACL_NAME	The name of the IP ACL	A string with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of IP ACL:

```
Switch# show access-list ip

ip access-list list_ipv4_1
 2 permit tcp host 1.1.1.1 any
 3 deny icmp any any
12 permit tcp any any
```

Related Commands

ip access-list

11.5 Extend ACL Commands

11.5.1 ip access-list extend

Command Purpose

Use this command to create extend IP ACL and then enter extend IP ACL configuration mode.
To remove this ACL, use the no form of this command.

Command Syntax

```
ip access-list ACL_NAME extend  
no ip access-list ACL_NAME extend
```

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	The name of an extend IP ACL	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has an extend IP ACL with the same name, this command will enter the extend IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.
When the name is not used by any ACL, this command is to create an extend IP ACL firstly and then enter the extend IP ACL configuration mode.
On how to apply the created extend IP ACL in the interface, please refer to the usage of match access-group command in related chapter.

Examples

This example shows how to create an extend IP ACL named list_ipv4_1 and then enter the extend IP ACL configuration mode:

```
Switch# configure terminal  
Switch(config)# ip access-list list_ipv4_1 extend  
Switch(config-ex-ip-acl)#
```

This example shows how to remove the extend IP ACL named list_ipv4_1:

```
Switch# configure terminal  
Switch(config)# no ip access-list list_ipv4_1 extend
```

Related Commands

match access-group

11.5.2 sequence-num

Command Purpose

Use this command to delete a filter from extend IP ACL.

Command Syntax

```
no sequence-num SEQUENCE_NUM
```

Parameter	Parameter Description	Parameter Value
<i>SEQUENCE_NUM</i>	The sequence number of an IP filter	1-131071

Command Mode

Extend IP ACL Configuration

Default

None

Usage

None

Examples

This example shows how to delete an IP or MAC filter with sequence number 10 from an extend IP ACL:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# no sequence-num 10
```

Related Commands

```
deny
deny udp
deny icmp
deny igmp
permit
permit tcp
permit udp
permit icmp
permit igmp
deny src-mac
permit src-mac
```

11.5.3 deny src-mac**Command Purpose**

Use this command to create a filter for discarding ongoing packets matching the filter rule.

Command Syntax

```
( SEQUENCE_NUM | ) deny src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR
MAC_ADDR_MASK | host MAC_ADDR ) | ( vlan VLAN_ID ) ( cos COS | ( inner-vlan INNER_VLAN_ID | ( inner-cos INNER_COS | ( arp-packet
( ( arp-op-code )
( sender-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ( target-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ) |
packet-length OPERATOR LENGTH | ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
any	Any host	-
MAC_ADDR MAC_ADDR_MASK	The MAC address and its wildcard bits	MAC and wildcard in HHHH.HHHH.HHHH format
host MAC_ADDR	The host with a specified MAC address	MAC address in HHHH.HHHH.HHHH format
dest-mac	Destination MAC address	-
VLAN_ID	VLAN-ID	1-4094
COS	CoS	0-7
INNER_VLAN_ID	Inner VLAN-ID	1-4094
INNER_COS	Inner CoS	0-7
arp	ARP protocol	-

Parameter	Parameter Description	Parameter Value
arp-op-code	arp-op-code	0-65535
sender-ip	sender-ip	-
target-ip	target-ip	-
IP_ADDR IP_ADDR_MASK	The ip address and wildcard bits	IPv4 Address and Mask
host IP_ADDR	The host with a specified ip address	IPv4 Address
TIME-RANGE-NAME	The time-range used by the extend IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110.

Examples

This example shows how to create a filter in extend IP ACL to deny the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in extend IP ACL to deny all the packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny src-mac any
```

This example shows how to create a filter in extend IP ACL to deny the packet whose source MAC address is between the ranges specified:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

11.5.4 permit src-mac

Command Purpose

Use this command to create a filter for allowing packets matching the filter rule to be delivered.

Command Syntax

```
( SEQUENCE_NUM | ) permit src-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) ( dest-mac ( any | MAC_ADDR MAC_ADDR_MASK | host MAC_ADDR ) | ) ( vlan VLAN_ID | ) ( cos VALUE | ) ( inner-vlan INNER_VLAN_ID | ) ( inner-cos INNER_COS | ) ( arp-packet ( ( arp-op-code ) ( sender-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ) ( target-ip ( IP_ADDR IP_ADDR_MASK | any | host IP_ADDR ) | ) ) | packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP Extend ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
any	Any host	-
MAC_ADDR MAC_ADDR_MASK	The MAC address and its wildcard bits	MAC and wildcard in HHHH.HHHH.HHHH format
host MAC_ADDR	The host with a specified MAC address	MAC address in HHHH.HHHH.HHHH format
dest-mac	Destination MAC address	-
VLAN_ID	VLAN-ID	1-4094
COS	CoS	0-7
INNER_VLAN_ID	Inner VLAN-ID	1-4094
INNER_COS	Inner CoS	0-7
arp	ARP protocol	-
arp-op-code	arp-op-code	0-65535
sender-ip	sender-ip	-
target-ip	target-ip	-
IP_ADDR IP_ADDR_MASK	The ip address and wildcard bits	IPv4 Address and Mask
host IP_ADDR	The host with a specified ip address	IPv4 Address
TIME-RANGE-NAME	The time-range used by the extend IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created MAC filter is 115.

Examples

This example shows how to create a filter in extend IP ACL to permit the packets with source MAC address 001A.A02C.A1DF:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-ac)# 1 permit src-mac host 001A.A02C.A1DF
This example shows how to create a filter in extend IP ACL to permit all the packets:
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-ac)# 2 permit src-mac any
This example shows how to create a filter in MAC ACL to permit the packets with source MAC address between the ranges specified:
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

11.5.5 Deny

Command Purpose

Use this command to discard ongoing IP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny ( PROTO_NUM | any ) ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP )
( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number, the range is 0 to 255	Agreement Number
any	Any protocol	-
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
host SRC_IP	The source IP address of a host	IPv4 Address
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration
0-255

Default

None

Usage

If an IP address wildcard bit is provided, the IP address is logically-anded in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created IP filter is 110.

Examples

This example shows how to create a filter in extend IP ACL to deny any IP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny any any any
```

This example shows how to create a filter in extend IP ACL to deny the fragment packets with the source IP addresss 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny any host 1.1.1.1 any fragments
```

This example shows how to create a filter in extend IP ACL to deny any routed packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny any any any routed-packet
```

Related Commands

no sequence-num

11.5.6 deny tcp

Command Purpose

Use this command to reject TCP packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny tcp (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (src-port *OPERATOR SRC_PORT* |) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (dst-port *OPERATOR DST_PORT* |) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (established | (match-any | match-all *FLAG-NAME* |)) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP Extend ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_IP	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_IP	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63

Parameter	Parameter Description	Parameter Value
established	Match established connections	-
match-any	Match any of the flag-name	-
FLAG-NAME	Match all the flag-name, including ack, fin, psh, rst, syn and urg	ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to deny any TCP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny tcp any any
```

This example shows how to create a filter in extend IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in extend IP ACL to deny any TCP packets in established TCP streams:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 3 deny tcp any any established
```

This example shows how to create a filter in extend IP ACL to deny the TCP ACK packets with the source IP address 10.10.10.10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

11.5.7 deny udp

Command Purpose

Use this command to reject UDP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny udp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( src-port OPERATOR SRC_PORT | ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP Extend ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_IP	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_IP	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the IP filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.5.8 deny icmp

Command Purpose

Use this command to reject ICMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny icmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( icmp-type TYPE_NUM ( icmp-code CODE_NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
TYPE_NUM	ICMP message type	0-255
CODE_NUM	ICMP message code	0-255
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	IPv4 Address
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-

Parameter	Parameter Description	Parameter Value
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny udp any any
```

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.5.9 deny igmp

Command Purpose

Use this command to reject IGMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny igmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( IGMP-TYPE | )
( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
IGMP-TYPE	IGMP type	including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to deny any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny icmp any any
```

This example shows how to create a filter in extend IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

11.5.10 deny gre**Command Purpose**

Use this command to reject GRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny gre (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (key *KEY* mask *KEY-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment |) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-

Parameter	Parameter Description	Parameter Value
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject GRE packets.

Examples

This example shows how to create a filter in extend IP ACL to deny any IGMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny igmp any any
```

This example shows how to create a filter in extend IP ACL to deny the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

11.5.11 deny nvgre

Command Purpose

Use this command to reject NVGRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) deny nvgre (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (vsid *VSID* mask *VSID-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment |) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
VSID	NVGRE vsid	0-16777215
VSID-MASK	NVGRE vsid mask	0-0xFFFFF

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to reject NVGRE packets.

Examples

This example shows how to create a filter in extend IP ACL to deny any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny gre any any key 0 mask 0
```

This example shows how to create a filter in extend IP ACL to deny the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny gre host 1.1.1.1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.5.12 Permit

Command Purpose

Use this command to permit packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit ( PROTO_NUM | any ) ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP )
( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number, the range is 0 to 255	0-255
any	Any protocol	-
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-

Parameter	Parameter Description	Parameter Value
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

If an IP address wildcard bit is provided, the IP address is logically-anded in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created IP filter is 115.

Examples

This example shows how to create a filter in extend IP ACL to deny any NVGRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 deny nvgre any any vsid 0 mask 0
```

This example shows how to create a filter in extend IP ACL to deny the NVGRE packets with the source IP address 1.1.1.1, any destination IP address and the nvgre vsid is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 deny gre host 1.1.1.1 any vsid 10 mask 0xfffff
```

This example shows how to create a filter in extend IP ACL to permit any routed packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 30 permit any any routed-packet
```

Related Commands

no sequence-num

11.5.13 permit tcp

Command Purpose

Use this command to permit TCP packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit tcp (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (src-port *OPERATOR SRC_PORT* |) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (dst-port *OPERATOR DST_PORT* |) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (established | (match-any | match-all *FLAG-NAME* |)) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP Extend ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host SRC_IP	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_IP	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
established	Match established connections	-
match-any	Match any of the flag-name	-
FLAG-NAME	Match all the flag-name, including ack, f in, psh, rst, syn and urg	ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the IP filter	-

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to permit any TCP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 10 permit tcp any any
```

This example shows how to create a filter in extend IP ACL to permit the TCP packets with the source IP address 1.1.1.1, and source port ranges from 0 to 100:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 20 permit tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in extend IP ACL to permit any TCP packets in established TCP streams:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 30 permit tcp any any established
```

This example shows how to create a filter in extend IP ACL to permit the TCP ACK packets with the source IP address 10.10.10.0:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

11.5.14 permit udp

Command Purpose

Use this command to permit UDP packets when the packets match this access-list.

Command Syntax

```
( SEQUENCE_NUM | ) permit udp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( src-port OPERATOR SRC_PORT | ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( dst-port OPERATOR DST_PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP Extend ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask

Parameter	Parameter Description	Parameter Value
any	Any source host	-
host SRC_IP	The source IP address of a host	IPv4 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address and Mask
host DST_IP	The destination IP address of a host	IPv4 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the IP filter	-
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 permit udp any any
```

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

11.5.15 permit icmp

Command Purpose

Use this command to permit ICMP packets when the packets match this access-list.

Command Syntax

```
( SEQUENCE_NUM | ) permit icmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
icmp-type TYPE-NUM	ICMP message type	0-255
icmp-code CODE-NUM	ICMP message code	0-255
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to permit any ICMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 permit icmp any any
```

This example shows how to create a filter in extend IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

None

11.5.16 permit igmp**Command Purpose**

Use this command to permit IGMP packets matching the IP filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit igmp ( SRC_IP SRC_IP_MASK | any | host SRC_IP ) ( DST_IP DST_IP_MASK | any | host DST_IP ) ( IGMP-TYPE | )
( ip-precedence PRECEDENCE | dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment )
( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
IGMP-TYPE	IGMP type	including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IP protocol number, the range is 0 to 255	0-255
any	Any protocol	-
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-

Parameter	Parameter Description	Parameter Value
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to permit any IGMP packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 permit igmp any any
```

This example shows how to create a filter in extend IP ACL to permit the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 permit igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

11.5.17 permit gre

Command Purpose

Use this command to permit GRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit gre (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (key *KEY* mask *KEY-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment |) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	IPv4 Address
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address

Parameter	Parameter Description	Parameter Value
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit GRE packets.

Examples

This example shows how to create a filter in extend IP ACL to permit any GRE packets:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 1 permit gre any any key 0 mask 0
```

This example shows how to create a filter in extend IP ACL to permit the GRE packets with the source IP address 1.1.1.1, any destination IP address and the gre key is 10:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# 2 permit gre host 1.1.1.1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.5.18 permit nvgre

Command Purpose

Use this command to permit NVGRE packets matching the IP filter.

Command Syntax

(*SEQUENCE_NUM* |) permit nvgre (*SRC_IP SRC_IP_MASK* | any | host *SRC_IP*) (*DST_IP DST_IP_MASK* | any | host *DST_IP*) (vsid *VSID* mask *VSID-MASK*) (ip-precedence *PRECEDENCE* | dscp *DSCP* |) (non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment |) (routed-packet |) (options |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
VSID	NVGRE vsid	0-16777215
VSID-MASK	NVGRE vsid mask,	0-0xFFFFF

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IP SRC_IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source IP address	-
host SRC_IP	The source IP address of a host	-
DST_IP DST_IP_MASK	The destination IP address and its wildcard bits	IPv4 Address
host DST_IP	The destination IP address of a host	IPv4 Address
PRECEDENCE	Match packets with given precedence value	0-7
DSCP	Match packets with given dscp value	0-63
non-fragment	Match packets with non fragment	-
first-fragment	Match packets with first fragment	-
non-or-first-fragment	Match packets with non first fragment	-
small-fragment	Match packets with small fragment	-
non-first-fragment	Match packets with non first fragment	-
routed-packet	Match routed packet	-
options	Match packets with IP options	-
TIME-RANGE-NAME	The time-range used by the filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

Extend IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit NVGRE packets.

Examples

This example shows how to create a filter in extend IP ACL to permit any NVGRE packets:

```
Switch# configure terminal
```

```
Switch(config)# ip access-list list_ipv4_1 extend
```

```
Switch(config-ex-ip-acl)# 1 permit nvgre any any vsid 0 mask 0
```

This example shows how to create a filter in extend IP ACL to permit the NVGRE packets with the source IP address 1.1.1.1, any destination IP address and the nvgre vsid is 10:

```
Switch# configure terminal
```

```
Switch(config)# ip access-list list_ipv4_1 extend
```

```
Switch(config-ex-ip-acl)# 2 permit gre host 1.1.1.1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.5.19 Remark

Command Purpose

Use this command to add remarks for the extend IP ACL.

To remove remarks from the extend IP ACL, use the no form of this command.

Command Syntax

remark *REMARK*
no remark

Parameter	Parameter Description	Parameter Value
REMARK	The remarks of the extend IP ACL	A string with up to 100 characters

Command Mode

Extend IP ACL Configuration

Default

None

Usage

The remark is up to 100 characters.

Examples

This example shows how to add a remark to describe the extend IP ACL:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# remark remard0flist1
```

This example shows how to remove the remark from the extend IP ACL:

```
Switch# configure terminal
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl)# no remark
```

Related Commands

None

11.5.20 show access-list ip extend

Command Purpose

Use this command to show the information of extend IP ACL.

Command Syntax

show access-list ip (*ACL_NAME* extend |)

Parameter	Parameter Description	Parameter Value
ACL_NAME extend	The name of the extend IP ACL	A string with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of extend IP ACL:

```
Switch# show access-list ip
```

```
ip access-list ex_ip_list_ipv4_1 extend
 2 permit tcp host 1.1.1.1 any
 3 deny icmp any any
12 permit tcp any any
```

Related Commands

ip access-list extend

11.6 ACLv6 Commands

11.6.1 ipv6 access-list

Command Purpose

Use this command to create IPv6 ACL and then enter IPv6 ACL in global configuration mode.

Command Syntax

ipv6 access-list *ACL_NAME*

no ipv6 access-list *ACL_NAME*

Parameter	Parameter Description	Parameter Value
ACL_NAME	The name of the IPv6 ACL	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IPv6 ACL with the same name, this command will enter the IPv6 ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the IPv6 ACL firstly and then enter the IPv6 ACL configuration mode.

Examples

This example shows how to create an IPv6 ACL named list_ipv6_1 and then enter the IPv6 ACL configuration mode:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)#
```

This example shows how to remove the IPv6 ACL named list_ipv6_1:

```
Switch# configure terminal
Switch(config)# no ipv6 access-list list_ipv6_1
```

Related Commands

match access-group

11.6.2 sequence-num

Command Purpose

Use this command to remove a filter from IPv6 ACL.

Command Syntax

no sequence-num *SEQUENCE_NUM*

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of a IPv6 filter	The range is 1 to 131071

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to remove a filter with the sequence-num 10 from IPv6 ACL:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# no sequence-num 10
```

Related Commands

deny

deny tcp

deny udp

deny icmp

permit

permit tcp

permit udp

permit icmp

11.6.3 remark

Command Purpose

Use this command to add remarks for the IPv6 ACL.

To remove remarks of the IPv6 ACL, use the no form of this command.

Command Syntax

remark *REMARK*

no remark

Parameter	Parameter Description	Parameter Value
REMARK	The remarks of the IPv6 ACL	String with up to 100 characters

Command Mode

IPv6 ACL Configuration

Default

None

Usage

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples

This example shows how to add a remark to describe the IPv6 ACL:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# remark remark of List for ipv6
```

This example shows how to remove the remark of the IPv6 ACL:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# no remark
```

Related Commands

ipv6 access-list

11.6.4 deny

Command Purpose

Use this command to discard ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IPv6 protocol number	0-255
any	Any IPv6 protocol	-
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length

Parameter	Parameter Description	Parameter Value
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

(*SEQUENCE_NUM* |) deny (*PROTO_NUM* | any) (*SRC_IPV6 SRC_IPV6_MASK* | any | host *SRC_IPV6*) (*DST_IPV6 DST_IPV6_MASK* | any | host *DST_IPV6*) (routed-packet |) (packet-length *OPERATOR LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Command Mode

IPv6 ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to deny any IPv6 packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny any any any
```

This example shows how to create a filter in IPv6 ACL to deny any routed packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny any any any routed-packet
```


Related Commands

no sequence-num

11.6.5 deny tcp

Command Purpose

Use this command to reject TCP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny tcp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6
DST_IPV6_MASK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | )
( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any destination host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
routed-packet	Match routed packet	-

Parameter	Parameter Description	Parameter Value
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any TCP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny tcp any any
```

This example shows how to create a filter in IPv6 ACL to deny the TCP packets with the source IPv6 address 2001::2020, source port 8080:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny tcp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

11.6.6 deny udp

Command Purpose

Use this command to reject UDP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny udp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6
DST_IPV6_MASK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | )
( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any destination host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any UDP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny udp any any
```

This example shows how to create a filter in IPv6 ACL to deny the UDP packets with the source IPv6 address 2001::2020, source port 8080:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny udp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

11.6.7 deny icmp**Command Purpose**

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny icmp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range
TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
TYPE-NUM	ICMP message type	0-255
CODE-NUM	ICMP message code	0-255
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address

Parameter	Parameter Description	Parameter Value
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any ICMP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny icmp any any
```

This example shows how to create a filter in IPv6 ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

11.6.8 deny gre**Command Purpose**

Use this command to reject GRE packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny gre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( flow-label FLOW-LABEL-VALUE | ) ( key KEY mask KEY-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment |
small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME
| )
```

Parameter	Parameter Description	Parameter Value
FLOW-LABEL-VALUE	Flow label	0-1048575
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny gre any any key 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny gre host 2000::1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.6.9 deny nvgre

Command Purpose

Use this command to reject NVGRE packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) deny nvgre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( flow-label FLOW-LABEL-VALUE | ) ( vsid VSID mask VSID-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment |
small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME
| )
```

Parameter	Parameter Description	Parameter Value
FLOW-LABEL-VALUE	Flow label	0-1048575
VSID	NVGRE VSID	0-16777215
VSID-MASK	NVGRE VSID MASK	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters

Parameter	Parameter Description	Parameter Value
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 deny nvgre any any vsid 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 deny gre host 2000::1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.6.10 permit**Command Purpose**

Use this command to permit ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE_NUM* |) permit (*PROTO_NUM* | any) (*SRC_IPV6* *SRC_IPV6_MASK* | any | host *SRC_IPV6*) (*DST_IPV6* *DST_IPV6_MASK* | any | host *DST_IPV6*) (routed-packet |) (packet-length *OPERATOR* *LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
PROTO_NUM	An IPv6 protocol number	0-255
any	Any IPv6 protocol	-
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address

Parameter	Parameter Description	Parameter Value
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR LENGTH	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to permit any IPv6 packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit any any any
```

This example shows how to create a filter in IPv6 ACL to permit any routed packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit any any any routed-packet
```

Related Commands

no sequence-num

11.6.11 permit tcp

Command Purpose

Use this command to permit TCP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit tcp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( src-port OPERATOR SRC_PORT | ) ( DST_IPV6
DST_IPV6_MASK | any | host DST_IPV6 ) ( dst-port OPERATOR DST_PORT | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | )
( time-range TIME-RANGE-NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any destination host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any TCP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit tcp any any
```

This example shows how to create a filter in IPv6 ACL to permit the TCP packets with the source IPv6 address 2001::2020, source port 8080:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit tcp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

11.6.12 permit udp

Command Purpose

Use this command to permit UDP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE_NUM* |) permit udp (*SRC_IPV6* *SRC_IPV6_MASK* | any | host *SRC_IPV6*) (src-port *OPERATOR* *SRC_PORT* |) (*DST_IPV6* *DST_IPV6_MASK* | any | host *DST_IPV6*) (dst-port *OPERATOR* *DST_PORT* |) (routed-packet |) (packet-length *OPERATOR* *LENGTH* |) (time-range *TIME-RANGE-NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK any	The source IPv6 prefix address Any destination host	IPv6 Address and mask length -
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
OPERATOR SRC_PORT	Source port operator and value	Source port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
DST_IPV6 DST_IPV6_MASK host DST_IPV6	The destination IPv6 prefix address The destination IPv6 address of a host	IPv6 Address and mask length IPv6 Address
OPERATOR DST_PORT	Destination port operator and value	Destination port, the range is 0-65535. Operator including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any UDP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit udp any any
```

This example shows how to create a filter in IPv6 ACL to permit the UDP packets with the source IPv6 address 2001::2020, source port 8080:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit udp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

11.6.13 permit icmp

Command Purpose

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit icmp ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( routed-packet | ) ( packet-length OPERATOR LENGTH | ) ( time-range
TIME-RANGE-NAME | )
```

For other parameter descriptions, see the description in the "permit" section above.

Parameter	Parameter Description	Parameter Value
icmp-type TYPE-NUM	ICMP message type	0-255
icmp-code CODE-NUM	ICMP message code	0-255
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any ICMP packets:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit icmp any any
```

This example shows how to create a filter in IPv6 ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3:

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

11.6.14 permit gre

Command Purpose

Use this command to permit GRE packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit gre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( flow-label FLOW-LABEL-VALUE | ) ( key KEY mask KEY-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment |
small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME
| )
```

For other parameter descriptions, see "deny gre" above.

Parameter	Parameter Description	Parameter Value
FLOW-LABEL-VALUE	Flow label	0-1048575
KEY	GRE key	0-4294967295
KEY-MASK	GRE key mask	0-0xFFFFFFFF
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length

Parameter	Parameter Description	Parameter Value
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length,operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit gre any any key 0 mask 0

Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any key 10 mask 0xffffffff
```

Related Commands

no sequence-num

11.6.15 permit nvgre

Command Purpose

Use this command to permit NVGRE packets matching the IPv6 filter.

Command Syntax

```
( SEQUENCE_NUM | ) permit nvgre ( SRC_IPV6 SRC_IPV6_MASK | any | host SRC_IPV6 ) ( DST_IPV6 DST_IPV6_MASK | any | host DST_IPV6 )
( flow-label FLOW-LABEL-VALUE | ) ( vsid VSID mask VSID-MASK ) ( dscp DSCP | ) ( non-fragment | first-fragment | non-or-first-fragment |
small-fragment | non-first-fragment | ) ( routed-packet | ) ( options | ) ( packet-length OPERATOR LENGTH | ) ( time-range TIME-RANGE-NAME
| )
```

For other parameter descriptions, see "deny nvgre" above.

Parameter	Parameter Description	Parameter Value
FLOW-LABEL-VALUE	Flow label	0-1048575
VSID	NVGRE VSID	0-16777215
VSID-MASK	NVGRE VSID MASK	0-0xFFFFF
SEQUENCE_NUM	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
SRC_IPV6 SRC_IPV6_MASK	The source IPv6 prefix address	IPv6 Address and mask length
any	Any source host	-
host SRC_IPV6	The source IPv6 address of a host	IPv6 Address
DST_IPV6 DST_IPV6_MASK	The destination IPv6 prefix address	IPv6 Address and mask length
host DST_IPV6	The destination IPv6 address of a host	IPv6 Address
routed-packet	Match routed packet	-
TIME-RANGE-NAME	The time-range used by the IPv6 filter	A string with up to 40 characters
OPERATOR	Packet length, operator including eq (equal to), lt (less than), gt (greater than), and range	eq (equal to), lt (less than), gt (greater than), and range
LENGTH	The length value	64-16382

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 1 permit nvgre any any vsid 0 mask 0
```

```
Switch# configure terminal
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)# 2 permit gre host 2000::1 any vsid 10 mask 0xfffff
```

Related Commands

no sequence-num

11.6.16 show access-list ipv6

Command Purpose

Use this command to show the IPv6 ACL information.

Command Syntax

show access-list ipv6 (*ACL_NAME* |)

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	The name of the IPv6 ACL	A string with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

If no ipv6 acl are specified, all ipv6 access-lists in the system should be shown.

Examples

This example shows how to show the IPv6 ACL information:

```
Switch# show access-list ipv6

ipv6 access-list list_ipv6_1
  10 deny any 2001::/48 any
  20 permit any any any
```

Related Commands

ipv6 access-list

11.7 Port Group Commands

11.7.1 port-group

Command Purpose

Use this command to create port group and then enter port group in global configuration mode. Use no port-group command to delete the port group.

Command Syntax

port-group *PORT_GROUP_NAME*

no port-group *PORT_GROUP_NAME*

Parameter	Parameter Description	Parameter Value
<i>PORT_GROUP_NAME</i>	The name of the port group	A string with up to 32 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has a port group with the same name, this command will enter the port group configuration mode.

When the name is not used by any port group, this command is to create the port group firstly and then enter the port group configuration mode.

Examples

This example shows how to create a port group named port_group_1 and then enter the port group configuration mode:

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)#
```

This example shows how to remove the port group named list_mac_1:

```
Switch# configure terminal
Switch(config)# no port-group port_group_1
```

Related Commands

None

11.7.2 member interface**Command Purpose**

Use this command to add a physical interface or an aggregation interface to port group. Use no member interface command to delete the physical interface or aggregation interface.

Command Syntax

member interface (IFPHYSICAL | IFAGG)

no member interface

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	The name of the physical interface	Support physical ports
IFAGG	The name of the aggregation interface	Support aggregation ports

Command Mode

Port-group Configuration

Default

None

Usage

If the interface is already an aggregation member interface, it cannot be added. If the interface has already been added to another port group, it cannot be added.

Examples

This example shows how to create a member interface :

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)# member interface eth-0-1
```

This example shows how to remove the member interface :

```
Switch# configure terminal
Switch(config)# port-group port_group_1
Switch(config-port-group)# no member interface eth-0-1
```

Related Commands

None

11.8 Vlan Group Commands

11.8.1 vlan-group

Command Purpose

Use this command to create vlan group and then enter vlan group in global configuration mode. Use no vlan-group command to delete the vlan group.

Command Syntax

vlan-group VLAN_GROUP_NAME

no vlan-group VLAN_GROUP_NAME

Parameter	Parameter Description	Parameter Value
VLAN_GROUP_NAME	The name of the vlan group	A string with up to 32 characters

Command Mode

Global Configuration

Default

None

Usage

If the system already has a vlan group with the same name, this command will enter the vlan group configuration mode.

When the name is not used by any vlan group, this command is to create the vlan group firstly and then enter the vlan group configuration mode.

Examples

This example shows how to create a vlan group named vlan_group_1 and then enter the vlan group configuration mode:

```
Switch# configure terminal
Switch(config)# vlan-group vlan_group_1
Switch(config-vlan-group)#
```

This example shows how to remove the vlan group named vlan_group_1:

```
Switch# configure terminal
Switch(config)# no vlan-group vlan_group_1
```

Related Commands

None

11.8.2 member vlan

Command Purpose

Use this command to add a vlan to vlan group. Use no member vlan command to delete the vlan.

Command Syntax

member vlan VLAN_ID

no member vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	The vlan id	1-4094

Command Mode

Vlan-group Configuration

Default

None

Usage

If the vlan has already been added to another vlan group, it cannot be added.

Examples

This example shows how to create a member vlan:

```
Switch# configure terminal
Switch(config)# vlan-group vlan_group_1
Switch(config-vlan-group)# member vlan 10
```

This example shows how to remove the member vlan :

```
Switch# configure terminal
Switch(config)# vlan-group vlan_group_1
Switch(config-vlan-group)# no member vlan 10
```

Related Commands

None

11.9 COPP Commands

11.9.1 control-plane access-list

Command Purpose

Use this command to create a control-plane access list.

Use the no form to delete the access list.

Command Syntax

control-plane access-list NAME

no control-plane access-list NAME

Parameter	Parameter Description	Parameter Value
NAME	Specify access list name	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to create a control-plane access list.:

```
Switch # configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)# quit
```

Related Commands

match access-group

11.9.2 (deny|permit) exception any

Command Purpose

Use deny command to discard any type of packets to the cpu.

Use permit command to let any type of packets to the cpu pass

Command Syntax

(SEQUENCE_NUM |) (deny | permit) exception any (time-range ? TIME_RANGE_NAME |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
TIME_RANGE_NAME	The time-range used by the IP filter	A string with up to 40 characters

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard any type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)# deny exception any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.3 (deny|permit) exception ipda**Command Purpose**

Use deny command to discard ipda type of packets to the cpu.

Use permit command to let ipda type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( ipv4 ) ( <0-255> | any ) ( IP_ADDR IP_MASK |
any | host IP_ADDR ) ( any ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( ipv4 ) ( icmp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( icmp-type IGMP_TYPE ( icmp-code ICMP_CODE | ) ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( ipv4 ) ( udp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( src-port ( eq L4_PORT | ) ) ( dst-port ( eq L4_PORT | ) ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( ipv4 ) ( gre ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } ) ( ipv6 ) ( <0-255> | any ) ( any ) ( any )
( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( icmp ) ( any ) ( any ) ( icmp-type
IGMP_TYPE ( icmp-code ICMP_CODE | ) ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( udp ) ( any ) ( any ) ( src-port ( eq
L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) ( deny | permit ) exception ipda ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( gre ) ( any ) ( any ) ( time-range
NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
VLAN_ID	VLAN ID	1-4094
COS	The range of cos is from 0 to 7	0-7
any	Any source host	-
host IP_ADDR	The source IP address of a host	IPv4 Address
eq	Equal to	-
ICMP_TYPE	Icmp type	0-255

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard ipda type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)# deny exception ipda
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.4 (deny|permit) exception fwd-to-cpu

Command Purpose

Use deny command to discard fwd-to-cpu type of packets to the cpu.

Use permit command to let fwd-to-cpu type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( <0-255> | any ) ( IP_ADDR
IP_MASK | any | host IP_ADDR ) ( any ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( icmp ) ( IP_ADDR IP_MASK | any
| host IP_ADDR ) ( any ) ( icmp-type IGMP_TYPE ( icmp-code ICMP_CODE | ) ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( tcp ) ( IP_ADDR IP_MASK | any |
host IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( udp ) ( IP_ADDR IP_MASK | any |
host IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( gre ) ( IP_ADDR IP_MASK | any |
host IP_ADDR ) ( any ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( <0-255> | any ) ( any ) ( any )
( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( icmp ) ( any ) ( any ) ( icmp-type
IGMP_TYPE ( icmp-code ICMP_CODE | ) ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( tcp ) ( any ) ( any ) ( src-port ( eq
L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( udp ) ( any ) ( any ) ( src-port
( eq L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception fwd-to-cpu ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( gre ) ( any ) ( any ) ( time-range
NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
VLAN_ID	The range of vlan id is from 1 to 4094	1-4094
COS	The range of cos is from 0 to 7	0-7
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any source host	-
host IP_ADDR	The source IP address of a host	IPv4 Address
eq	Equal to	-
ICMP_TYPE	ICMP type	0-255
ICMP_CODE	The range of icmp-code is from 0-255	0-255

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard fwd-to-cpu type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception fwd-to-cpu
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.5 (deny|permit) exception slow-protocol

Command Purpose

Use deny command to discard slow-protocol type of packets to the cpu.

Use permit command to let slow-protocol type of packets to the cpu pass

Command Syntax

(*SEQUENCE_NUM* |) deny | permit exception slow-protocol (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception slow-protocol (sub-type *TYPE*) (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception slow-protocol (efm | lacp | synce) (time-range *NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
TYPE	The range of sub-type is from 0 to 255	0-255
efm	efm type message	-
lacp	lacp type message	-
synce	synce type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard slow-protocol type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception slow-protocol
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.6 (deny|permit) exception dhcp

Command Purpose

Use deny command to discard dhcp type of packets to the cpu.

Use permit command to let dhcp type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception dhcp ( time-range NAME | ) ( SEQUENCE_NUM | ) deny | permit exception dhcp ( dhcp )
( IP_ADDR IP_MASK | any | host IP_ADDR ) ( any ) ( client | server | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception dhcp ( dhcpv6 ) ( any ) ( any ) ( reply | request | ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
client	dhcp request type message	-
server	dhcp reply type message	-
request	dhcp client type message	-
reply	dhcp server type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard dhcp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception dhcp dhcp any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.7 (deny|permit) exception rip

Command Purpose

Use deny command to discard rip type of packets to the cpu.

Use permit command to let rip type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception rip ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception rip ( rip ) ( IP_ADDR IP_MASK | any | host IP_ADDR ) ( any ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception rip ( ripng ) ( any ) ( any ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP[address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard rip type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
```

```
Switch (config-cp-acl)#deny exception rip rip any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.8 (deny|permit) exception ospf

Command Purpose

Use deny command to discard ospf type of packets to the cpu.

Use permit command to let ospf type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception ospf ( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception ospf ( ospfv2 ) ( IP_ADDR IP_MASK | any | host IP_ADDR ) ( any ) ( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception ospf ( ospfv3 ) ( any ) ( any ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
ospfv2	ospfv2 type message	-
ospfv3	ospfv3 type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard ospf type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception ospf ospfv2 any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.9 (deny|permit) exception pim

Command Purpose

Use deny command to discard pim type of packets to the cpu.

Use permit command to let pim type of packets to the cpu pass

Command Syntax

(*SEQUENCE_NUM* |) deny | permit exception pim (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception pim (pim) (*IP_ADDR IP_MASK* | any | host *IP_ADDR*) (any) (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception pim (pimv6) (any) (any) (time-range *NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
pimv6	pimv6 type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard pim type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)# deny exception pim pim any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.10 (deny|permit) exception bgp

Command Purpose

Use deny command to discard bgp type of packets to the cpu.

Use permit command to let bgp type of packets to the cpu pass

Command Syntax

(*SEQUENCE_NUM* |) deny | permit exception bgp (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception bgp (bgp) (*IP_ADDR IP_MASK* | any | host *IP_ADDR*) (any) (time-range *NAME* |)

(*SEQUENCE_NUM* |) deny | permit exception bgp (bgp4plus) (any) (any) (time-range *NAME* |)

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
bgp4plus	bgp4plus type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard bgp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception bgp bgp any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.11 (deny|permit) exception vrrp

Command Purpose

Use deny command to discard vrrp type of packets to the cpu.

Use permit command to let vrrp type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception vrrp ( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception vrrp ( vrrp ) ( IP_ADDR IP_MASK | any | host IP_ADDR ) ( any ) ( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception vrrp ( vrrpv6 ) ( any ) ( any ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
vrrpv6	vrrpv6 type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard vrrp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception vrrp vrrp any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.12 (deny|permit) exception ssh

Command Purpose

Use deny command to discard ssh type of packets to the cpu.

Use permit command to let ssh type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception ssh ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception ssh ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( tcp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard ssh type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception ssh
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.13 (deny|permit) exception telnet

Command Purpose

Use deny command to discard telnet type of packets to the cpu.

Use permit command to let telnet type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception telnet ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception telnet ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( tcp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard telnet type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception telnet
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.14 (deny|permit) exception tcp

Command Purpose

Use deny command to discard tcp type of packets to the cpu.

Use permit command to let tcp type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception tcp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception tcp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( tcp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception tcp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( ipv6 ) ( tcp ) ( any ) ( any ) ( src-port ( eq
L4_PORT ) | ) ( dst-port ( eq L4_PORT ) | ) ( time-range NAME | )
```


Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard tcp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception tcp
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.15 (deny|permit) exception mlag**Command Purpose**

Use deny command to discard mlag type of packets to the cpu.

Use permit command to let mlag type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception mlag ( untag-vlan { vlan VLAN_ID | cos COS } | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception mlag ( untag-vlan { vlan VLAN_ID | cos COS } | ) ( ipv4 ) ( tcp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( src-port ( eq L4_PORT ) | ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
SEQUENCE_NUM	The sequence number of the filter in CoPP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented.	1-131071
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address

Command Mode

Control plane Configuration

Default

None

Usage

None

Examples

The following example shows how to discard mlag type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception mlag
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.16 (deny|permit) exception arp

Command Purpose

Use deny command to discard arp type of packets to the cpu.

Use permit command to let arp type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception arp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( arp-op-code ARP_OP_CODE | ) ( sender-ip
(IP_ADDR IP_MASK | any | host IP_ADDR ) | ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception arp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( garp ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception arp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( arp-reply | arp-request ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception arp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( rarp-reply | rarp-request ) ( time-range NAME
| )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
VLAN_ID	The range of vlan id is from 1 to 4094	1-4094
COS	The range of cos is from 0 to 7	0-7
ARP_OP_CODE	The range of arp-op-code is from 0 to 65535	0-65535
arp-request	Arp request type message	-
arp-reply	Arp reply type message	-
rarp-request	Rarp request type message	-
rarp-reply	Rarp reply type message	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard arp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception arp arp-op-code 1 any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.17 (deny|permit) exception igmp**Command Purpose**

Use deny command to discard igmp type of packets to the cpu.

Use permit command to let igmp type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) ( deny | permit ) exception igmp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( igmp ) ( IP_ADDR IP_MASK | any | host IP_ADDR ) ( any ) ( dvmrp | host-query | host-report | mtrace | mtrace-response | pim | precedence | trace | v2-leave | v2-report | v3-report | ) ( time-range NAME | )
```

```
( SEQUENCE_NUM | ) deny | permit exception igmp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( igmp ) ( IP_ADDR IP_MASK | any | host
IP_ADDR ) ( any ) ( igmp-type IGMP_TYPE ) ( time-range NAME | )
( SEQUENCE_NUM | ) deny | permit exception igmp ( untag-vlan | { vlan VLAN_ID | cos COS } | ) ( mld ) ( any ) ( any ) ( mld-query | mld-report |
mld-done | mldv2-report | ) ( time-range NAME | )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask
any	Any IP address	-
host IP_ADDR	The source IP address of a host	IPv4 Address
VLAN_ID	The range of vlan id is from 1 to 4094	1-4094
COS	The range of cos is from 0 to 7	0-7
IGMP_TYPE	The range of icmp-type is from 0 to 255	0-255
dvmrp	Dvmrp type message	-
host-query	host-query type message	-
host-report	host-report type message	-
mtrace	mtrace type message	-
mtrace-response	mtrace-response type message	-
pim	pim type message	-
trace	trace type message	-
v2-leave	v2-leave type message	-
v2-report	v2-report type message	-
v3-report	v3-report type message	-
mld-query	Multicast Listener Query(130)	-
mld-report	Multicast Listener Report(131)	-
mld-done	Multicast Listener Done(132)	-
mldv2-report	MLDv2 Multicast Listener Report(143)	-

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard igmp type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
```

```
Switch (config-cp-acl)#deny exception igmp igmp any any
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.18 (deny|permit) exception

Command Purpose

Use deny command to discard specified type of packets to the cpu.

Use permit command to let specified type of packets to the cpu pass

Command Syntax

```
( SEQUENCE_NUM | ) deny | permit exception ( bpdv | erps | eapol | smart-link | ldp | ptp | rsvp | icmp-redirect | mcast-rpf-fail |
macsa-mismatch | vlan-security-discard | port-security-discard | ip-option | udd | dot1x-mac-bypass | l2protocol-tunnel ) ( time-range
NAME | )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR IP_MASK	The source IP address and its wildcard bits	IPv4 Address and Mask

Command Mode

Config-cp-acl

Default

None

Usage

None

Examples

The following example shows how to discard pbdu type of packets to the cpu.:

```
Switch# configure terminal
Switch (config)# control-plane access-list test
Switch (config-cp-acl)#deny exception bpdv
Switch (config-cp-acl)#
```

Related Commands

Control-plane access-list

11.9.19 class-map type (control-plane)

Command Purpose

Use this command to create a control-plane class map.

Use the no form to delete the class map.

Command Syntax

class-map type (control-plane) NAME

no class-map NAME

Parameter	Parameter Description	Parameter Value
NAME	Specify class map name	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to create a control-plane class map.:

```
Switch # configure terminal
Switch (config)# class-map type control-plane test
Switch (config-cmap-cp)
```

Related Commands

class type control-plane

11.9.20 policy-map type (control-plane)**Command Purpose**

Use this command to create a control-plane policy map.

Use the no form to delete the policy map.

Command Syntax

policy-map type (control-plane) NAME

no policy-map NAME

Parameter	Parameter Description	Parameter Value
NAME	Specify policy map name	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to create a control-plane policy map.:

```
Switch # configure terminal
Switch (config)# policy-map type control-plane test
Switch (config-pmap-cp)#
```

Related Commands

service-policy type control-plane input

11.9.21 class type control-plane**Command Purpose**

Use this command to add the class map to the policy map

Use the no form of this command to unbind it.

Command Syntax

class type control-plane (NAME | class-default)

no class type control-plane (NAME | class-default)

Parameter	Parameter Description	Parameter Value
NAME	Specify class map name	A string with up to 40 characters

Command Mode

Config-pmap-c Configuration

Default

None

Usage

None

Examples

The following example shows how to add the class map to the policy map:

```
Switch# configure terminal
Switch (config)# policy-map type control-plane test
Switch (config-pmap-cp)# class type control-plane test
Switch (config-pmap-cp-c)#
```

Related Commands

class-map type (control-plane)

11.9.22 statistics enable

Command Purpose

Use this command to enable statistics.

Use the no form to disable it.

Command Syntax

statistics enable

no statistics enable

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to enable statistics.:

```
Switch# configure terminal
Switch (config)# policy-map type control-plane test
Switch (config-pmap-cp)# class type control-plane test
Switch (config-pmap-cp-c)# statistics enable
```

Related Commands

class-map type (control-plane)

11.9.23 control-plane

Command Purpose

Use this command to enter global control plane mode.

Command Syntax

control-plane

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following example shows how to enter global control plane mode:

```
Switch# configure terminal
Switch (config)# control-plane
Switch (Config-control-plain)#
```

Related Commands

service-policy type control-plane input

11.9.24 service-policy type control-plane input**Command Purpose**

Use this command to apply the control plane policy.

Use the no form of this command to remove it.

Command Syntax

```
service-policy type control-plane input NAME
no service-policy type control-plane input
```

Parameter	Parameter Description	Parameter Value
NAME	Specify policy input name	A string with up to 40 characters

Command Mode

Control plane Configuration

Default

None

Usage

None

Examples

The following example shows how to apply the control plane policy:

```
Switch# configure terminal
Switch (Config-control-plain)# service-policy type control-plane input test
Switch (Config-control-plain)#
```

Related Commands

policy-map type control-plane

11.9.25 show policy-map type control-plane statistics input ace

Command Purpose

Use this command to show stats of copp policer

Command Syntax

show policy-map type control-plane statistics input ace (class-based | ace-based) (class NAME |)

Parameter	Parameter Description	Parameter Value
NAME	Specify class map name	A string with up to 40 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to show stats of copp policer:

```
Switch # show policy-map type control-plane statistics input policer
```

Related Commands

clear policy-map type control-plane statistics input

11.9.26 policer cir

Command Purpose

To Specify a policer for the classified traffic, config CIR CBS and enable policer statistics

Command Syntax

policer cir CIR (cbs CBS |) (statistics |)

Parameter	Parameter Description	Parameter Value
CIR	CIR Commit Information Rate (pps)	0-148809523
CBS	CBS - Commit Burst Size (packets) (default value is 4400)",	0-7600
statistics	enable policer stat	-

Command Mode

Config-pmap-c Configuration

Default

4400

Usage

limit the rate of some exception traffic to cpu

Examples

config the traffic rate of ARP exception and enable policer stat:

```
Switch# configure terminal
Switch(config)#control-plane access-list testacl
Switch(config-cp-acl)#10 permit exception arp
Switch(config-cp-acl)#class-map type control-plane testclass
Switch(config-cmap-cp)#match access-group testacl
Switch(config-cmap-cp)#policy-map type control-plane testpolicy
Switch(config-pmap-cp)#class type control-plane testclass
Switch(config-pmap-cp-c)#policer cir 100 statistics
Switch(config-pmap-cp-c)#control-plane
Switch(Config-control-plain)service-policy type control-plane input testpolicy
```

Related Commands

show policy-map type control-plane statistics input

11.9.27 show policy-map type control-plane statistics input policer**Command Purpose**

To show statistics of any policy, class name can be specified

Command Syntax

show policy-map type control-plane statistics input policer (class NAME |)

clear policy-map type control-plane statistics input policer

Parameter	Parameter Description	Parameter Value
NAME	Specify class map name	A string with up to 40 characters

Command Mode

Global Configuration

Default

None

Usage

To show statistics of any policy, class name can be specified

Examples

To show statistics of any policy, class name can be specified:

```
Switch#show policy-map type control-plane statistics input policer
```

Related Commands

policer cir

11. 10 IEEE 802.1x Commands

11.10.1 dot1x system-auth-ctrl

Command Purpose

Use the dot1x system-auth-ctrl to globally start the dot1x authenticate control feature.

To remove this configure, use no form of this command.

Command Syntax

dot1x system-auth-ctrl

no dot1x system-auth-ctrl

Command Mode

Global Configuration

Default

Disable

Usage

Use this command to globally start the dot1x feature. To make the dot1x configures on each port work normally, this command should be used.

Examples

The following is sample output from the dot1x system-auth-ctrl command:

```
Switch# configure terminal
Switch(config)# dot1x system-auth-ctrl
Switch(config)# no dot1x system-auth-ctrl
```

Related Commands

show dot1x

dot1x port-control

11.10.2 dot1x initialize

Command Purpose

Use the dot1x initialize privileged EXEC command on the switch to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

Command Syntax

dot1x initialize interface IFNAME

Parameter	Parameter Description	Parameter Value
IFNAME	Specify the interface name to be initialized	This function supports routed port and access port, and Does not Support trunk port

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following is sample output from the dot1x initialize command:

```
Switch# dot1x initialize interface eth-0/1
```

Related Commands

show dot1x

11.10.3 dot1x max-req

Command Purpose

Use the dot1x max-reauth-req interface configuration command on the switch to set the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state. Use the no form of this command to return to the default setting.

Command Syntax

dot1x max-req COUNT

no dot1x max-req

Parameter	Parameter Description	Parameter Value
COUNT	Number of times that the switch restarts the authentication process before the port changes to the unauthorized state.	1-10

Command Mode

Interface Configuration

Default

The default value of dot1x max-reauth-req is 2 times.

Usage

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following is sample output from the dot1x max-reauth-req command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x max-req 4
```

Related Commands

show dot1x

11.10.4 dot1x port-control

Command Purpose

Use the dot1x port-control interface configuration command on the switch to enable manual control of the authorization state of the port. Use the no form of this command to return to the default setting.

Support config dot1x in routed port, while can't config it in a logical port such as agg, and so on.

Command Syntax

dot1x port-control (auto | force-authorized | force-unauthorized | dir (both | in))

no dot1x port-control

Parameter	Parameter Description	Parameter Value
auto	Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client	-
force-authorized	Disable IEEE 802.1x authentication on the port and cause the port to transition to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client	-
force-unauthorized	Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port	-
dir	Specify the dot1x control direction	-
both	Discard received and transmitted packets	-
in	Discard received packets only	-

Command Mode

Interface Configuration

Default

Dot1x port control is disabled by default.

The default value of the control direction is "in".

Usage

You must globally enable IEEE 802.1x authentication on the switch by using the dot1x system-auth-control global configuration command before enabling IEEE 802.1x authentication on a specific port.

Examples

The following is sample output from the dot1x port-control command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x port-control auto
```

Related Commands

show dot1x

11.10.5 dot1x protocol-version

Command Purpose

Use the dot1x protocol-version interface configuration command on the switch to set the version of EAPOL packets. Use the no form of this command to return to the default setting.

Command Syntax

dot1x protocol-version *VER*
no dot1x protocol-version

Parameter	Parameter Description	Parameter Value
VER	The EAPOL version	1-2

Command Mode

Interface Configuration

Default

The default value of EAPOL version is 2.

Usage

You must specify the control of the authorization state of the port by the dot1x port-control command, before setting the EAPOL version.

Examples

The following is sample output from the dot1x protocol-version command:


```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# dot1x protocol-version 1
```

Related Commands

show dot1x

11.10.6 dot1x timeout quiet-period

Command Purpose

Use the dot1x timeout quiet-period interface configuration command on the switch to set the quiet time interval. Use the no form of this command to return to the default setting.

Command Syntax

dot1x timeout quiet-period *SECONDS*

no dot1x timeout quiet-period

Parameter	Parameter Description	Parameter Value
	The time interval (in seconds)	
SECONDS	between the retrials of authentication	1-65535 seconds

Command Mode

Interface Configuration

Default

The default value of dot1x quite-period is 60 seconds.

Usage

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

Examples

The following is sample output from the dot1x quiet-period command:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# dot1x timeout quiet-period 100
```

Related Commands

show dot1x

11.10.7 dot1x reauthentication

Command Purpose

Use the dot1x reauthentication interface configuration command on the switch to enable periodic re-authentication of the client. Use the no form of this command to return to the default setting.

Command Syntax

```
dot1x reauthentication
no dot1x reauthentication
```

Command Mode

Interface Configuration

Default

None

Usage

The default setting of dot1x re-authentication is disabled. when the re-authentication is disabled, the configuration of the re-authenticate timeout should not take effect.

Examples

The following is sample output from the dot1x reauthentication command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x reauthentication
```

Related Commands

```
show dot1x
dot1x timeout
```

11.10.8 dot1x re-authenticate

Command Purpose

Use the dot1x re-authenticate privileged EXEC command on the switch stack to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

Command Syntax

dot1x re-authenticate interface *IFNAME*

Parameter	Parameter Description	Parameter Value
IFNAME	The interface to re-authenticate	This function supports routed port and access port, and Does not Support trunk port

Command Mode

Privileged EXEC

Default

None

Usage

You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.

Examples

The following is sample output from the dot1x re-authenticate command:

```
Switch# dot1x re-authenticate interface eth-0-1
```

Related Commands

show dot1x

11.10.9 dot1x timeout

Command Syntax

dot1x timeout (re-authperiod *SECONDS* | server-timeout *SECONDS* | supp-timeout *SECONDS* | tx-period *SECONDS*)

no dot1x timeout (reauth-period | server-timeout | supp-timeout | tx-period)

Parameter	Parameter Description	Parameter Value
re-authperiod SECONDS	Set the number of seconds between reauthentication attempts.	60-65535 seconds
server-timeout SECONDS	Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server.	1-65535 seconds

Parameter	Parameter Description	Parameter Value
supp-timeout SECONDS	Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client.	1-65535 seconds
tx-period SECONDS	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.	1-65535 seconds

Command Mode

Interface Configuration

Default

None

Command Purpose

Use the dot1x timeout interface configuration command on the switch stack or on a standalone switch to set IEEE 802.1x timers. Use the no form of this command to return to the default setting.

Usage

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The dot1x timeout re-authperiod interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the dot1x reauthentication interface configuration command.

The default value of re-authperiod is 3600 seconds.

The default value of tx-period is 30 seconds.

The default value of supp-timeout is 30 seconds.

The default value of server-timeout is 30 seconds.

Examples

The following is sample output from the dot1x timeout command:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

Related Commands

dot1x reauthentication

show dot1x

11.10.10 dot1x guest-vlan

Command Purpose

Use the dot1x guest-vlan interface configuration command to specify an active VLAN as an 802.1x guest VLAN. Use the no form of this command to return to the default setting.

Command Syntax

dot1x guest-vlan *VLAN_ID*

no dot1x guest-vlan

Parameter	Parameter Description	Parameter Value
VLAN_ID	Specify an active VLAN as an 802.1x guest VLAN.	2-4094

Command Mode

Interface Configuration

Default

No guest VLAN is configured.

Usage

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame. Clients that are 802.1x-capable but fail authentication are not granted access to the network.

The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports

Examples

This example shows how to specify VLAN 5 as an 802.1x guest VLAN:

```
Switch# configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 5
Switch(config-vlan)#exit
Switch(config)# interface eth-0-1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x guest-vlan 5
```

Related Commands

show dot1x

11.10.11 show dot1x

Command Purpose

Use the show dot1x user EXEC command to display IEEE 802.1x session configuration, administrative status, and operational status for the switch or for the specified port.

Command Syntax

show dot1x interface *IFNAME*

show dot1x session brief ((interface *IFPHYSICAL* (mac *MACADDR* |)))

show dot1x (all |)

Parameter	Parameter Description	Parameter Value
IFNAME	Specify an interface	Support physical ports
MACADDR	Specify mac address	MAC Address in HHHH.HHHH.HHHH format
all	Display IEEE 802.1x information of all interfaces	-

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following is sample output from the show dot1x command:

```
Switch# show dot1x all
```

```
DUT1# show dot1x all
```

```
802.1X Port-Based Authentication Enabled
```

```
=====
```

```
802.1X info for interface eth-0-2
```

```
portEnabled      : false
```

```
portControl      : Auto
```

```
portMode         : Port based
```

```

portStatus          : Unauthorized
Mac Auth bypass     : disabled
reAuthenticate       : enabled
reAuthPeriod        : 3600
Max user number     : 255
Current session number : 0
Accept user number  : 0
Reject user number   : 0
Guest VLAN          : N/A
Assign VLAN         : N/A
QuietPeriod         : 60
ReqMax              : 2
TxPeriod            : 30
SuppTimeout         : 30
ServerTimeout       : 30
CD: adminControlledDirections : in
CD: operControlledDirections  : in
CD: bridgeDetected           : false
=====

```

Related Commands

```

dot1x system-auth-ctrl
dot1x port-control

```

11.10.12 show dot1x statistics

Command Purpose

Use the show dot1x user EXEC command to display IEEE 802.1x EAPOL packets statistics, for the switch or for the specified port.

Command Syntax

```

show dot1x statistics interface IFNAME
show dot1x statistics ( all | )

```

Parameter	Parameter Description	Parameter Value
IFNAME	Specify an interface	Support physical ports
all	Display IEEE 802.1x information of all interfaces	-

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following is sample output from the show dot1x command:

```
Switch# show dot1x statistics interface eth-0-1
```

```
802.1X statistics for interface eth-0-1
```

```
  EAPOL Frames Rx: 0 - EAPOL Frames Tx: 323
```

```
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
```

```
  EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
```

```
  EAP Req/Id Frames Tx: 241 - EAP Request Frames Tx: 0
```

```
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
```

```
  EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000
```

Related Commands

```
dot1x system-auth-ctrl
```

```
dot1x port-control
```

11.10.13 debug dot1x**Command Purpose**

Use this command to turn on the debug switches of dot1x module.

To restore the default, use the no form of this command

Command Syntax

```
debug dot1x ( event | timer | packet | all )
```

```
no debug dot1x ( event | timer | packet | all )
```

Parameter	Parameter Description	Parameter Value
event	put out the debug message of dot1x events	-
timer	put out the debug message of dot1x timer information	-
packet	put out the debug message of dot1x packets information, include sent and received	-

Parameter	Parameter Description	Parameter Value
all	put out all debug message mentioned above	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.

Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dot1x debug switches:

```
Switch# debug dot1x all
```

Related Commands

terminal monitor

show logging buffer

11.10.14 clear dot1x**Command Purpose**

Use the clear dot1x user EXEC command to clear the IEEE 802.1x statistics for the switch or for the specified port.

Command Syntax

clear dot1x statistics (all |)

Parameter	Parameter Description	Parameter Value
all	Display IEEE 802.1x information of all interfaces	-

Command Mode

Privileged EXEC

Default

None

Usage

Use the command "clear dot1x" to clear the IEEE 802.1x statistics for the switch or for the specified port.

Use the command "show dot1x" to display the IEEE 802.1x statistics.

Examples

The following is sample to using the clear dot1x command:

```
Switch# clear dot1x statistics
```

```
Switch# clear dot1x session-statistics
```

Related Commands

dot1x system-auth-ctrl

dot1x port-control

show dot1x

11.10.15 dot1x port-mode

Command Purpose

Use the "dot1x port-mode" command to set control mode of the interface.

Use the no form of this command to restore the default value.

Command Syntax

dot1x port-mode (port | mac)

no dot1x port-mode

Parameter	Parameter Description	Parameter Value
port	Set dot1x port based	-
mac	Set dot1x mac based	-

Command Mode

Interface Configuration

Default

By default the mode is port based.

Usage

Use the "dot1x port-mode" command to set control mode of the interface.

Use the no form of this command to restore the default value.

dot1x port-control must be enabled before set the control mode.

The control mode cannot be changed if there are users on line.

Examples

The following is a sample to use the dot1x port-mode command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x port-mode mac
```

Related Commands

dot1x port-control

11.10.16 dot1x max-user

Command Purpose

Use the "dot1x max-user" command to set max user of the interface.

Use the no form of this command to restore the default value.

Command Syntax

dot1x max-user *COUNT*

no dot1x max-user

Parameter	Parameter Description	Parameter Value
COUNT	Max user number of the port	1-255

Command Mode

Interface Configuration

Default

By default the user number is uncontrolled on port. The max number is according to the system hardware profile.

Usage

Use the "dot1x max-user" command to set max user of the interface.

Use the no form of this command to restore the default value.

dot1x port-control must be enabled before set the max value.

If there are users online, the set value should be larger than or at least be same as the users count.

The set value cannot be larger than the hardware resource count.

This count should limit the number of dot1x mac based user in state "accept", "reject" and "reauth", which should use hardware table for forwarding or discarding. The total number of users include "waiting" states should be 2 times as this configuration.

Examples

The following is a sample to use the dot1x max-user command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dot1x max-user 10
```

Related Commands

dot1x port-control

11.10.17 dot1x re-active radius-server

Command Purpose

Use the "dot1x re-active" command to active the specified radius servers.

Command Syntax

dot1x re-active radius-server (host *HOST_IP_ADDR* (auth-port *PORT* |) | interface *IFNAME* | all)

Parameter	Parameter Description	Parameter Value
host HOST_IP_ADDR	Re-active the radius-server by server ip	IPv4 Address
PORT	Re-active the radius-server by server ip and udp port. If the auth port is not specified the default port is 1812.	1-65535
IFNAME	Re-active the radius-servers by IEEE 802.1x client's interface	This function supports routed port and access port, and Does not Support trunk port
all	Re-active all radius-servers	-

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to active the radius server. Users do not need the wait for the radius-server dead time with this command.

Examples

The following is samples to use the dot1x re-active radius-server command:

```
Switch# dot1x re-activate radius-server
Switch# dot1x re-activate radius-server host 3.3.3.3 auth-port 1812
Switch# dot1x re-activate radius-server interface eth-0-9
```

Related Commands

radius-server host
radius-server deadtime
show radius-server

11. 11 Arp Inspection Commands

11.11.1 show ip arp inspection

Command Purpose

Use this command to display the configuration of arp inspection.

Command Syntax

```
show ip arp inspection
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to display the information of arp inspection:

Switch# show ip arp inspection

Source Mac Validation : Disabled

Destination Mac Validation : Disabled

IP Address Validation : Disabled

Vlan	Configuration	ACL Match	Static ACL
1	enabled	acl	
Vlan	ACL Logging	DHCP Logging	
1	deny	deny	
Vlan	Forwarded	Dropped	DHCP Drops ACL Drops
1	0	0	0
Vlan	DHCP Permits	ACL Permits	Source MAC Failures
1	0	0	0
Vlan	Dest MAC Failures	IP Validation Failures	Invalid Protocol Data
1	0	0	0

Related Commands

ip arp inspection vlan

11.11.2 show ip arp inspection interfaces

Command Purpose

Use this command to display the arp inspection configuration of specified interface.

Command Syntax

show ip arp inspection interfaces (*IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical/aggregation /loopback/vlan/tunnel ports

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to show the arp inspection configuration on interface.

Examples

This example shows how to display all the arp inspection configuration of all interface.:

```
Switch# show ip arp inspection interfaces
```

Interface	Trust State
=====	
eth-0-1	untrusted
eth-0-2	untrusted
eth-0-3	untrusted
eth-0-4	untrusted
eth-0-5	untrusted
eth-0-6	untrusted
eth-0-7	untrusted
eth-0-8	untrusted
eth-0-9	untrusted
eth-0-10	untrusted
eth-0-11	untrusted
eth-0-12	untrusted
eth-0-13	untrusted
eth-0-14	untrusted
eth-0-15	untrusted
eth-0-16	untrusted
eth-0-17	untrusted
eth-0-18	untrusted
eth-0-19	untrusted
eth-0-20	untrusted
eth-0-21	untrusted
eth-0-22	untrusted
eth-0-23	untrusted
eth-0-24	untrusted
eth-0-25	untrusted
eth-0-26	untrusted
eth-0-27	untrusted
eth-0-28	untrusted
eth-0-29	untrusted
eth-0-30	untrusted
eth-0-31	untrusted
eth-0-32	untrusted
eth-0-33	untrusted

```
eth-0-34      untrusted
eth-0-35      untrusted
eth-0-36      untrusted
eth-0-37      untrusted
eth-0-38      untrusted
eth-0-39      untrusted
eth-0-40      untrusted
eth-0-41      untrusted
eth-0-42      untrusted
eth-0-43      untrusted
eth-0-44      untrusted
eth-0-45      untrusted
eth-0-46      untrusted
eth-0-47      untrusted
eth-0-48      untrusted
```

Related Commands

ip arp inspection trust

11.11.3 show ip arp inspection log

Command Purpose

Use this command to display the log configuration and log information in arp inspection log buffer. The default number is 32.

Command Syntax

show ip arp inspection log (*NUMBER* |)

Parameter	Parameter Description	Parameter Value
NUMBER	Specify the number of message	1-1024

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to verify arp inspection log settings.

Examples

This example shows how to display the log information in arp inspection log buffer.:


```
Switch# show ip arp inspection log
```

```
Total Log Buffer Size : 32
```

```
Syslog rate : 5 entries per 1 seconds.
```

```
No entries in log buffer
```

Related Commands

```
ip arp inspection log-buffer
```

11.11.4 show ip arp inspection statistics

Command Purpose

Use this command to displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified vlan. If no vlans are specified or if a range is specified, displays information only for vlans with ARP Inspection enabled.

Command Syntax

```
show ip arp inspection statistics ( vlan VLAN_RNG_STR | )
```

Parameter	Parameter Description	Parameter Value
vlan <i>VLAN_RNG_STR</i>	Selected vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN.

Examples

This example shows how to display the arp inspection statistics:

```
Switch# show ip arp inspection statistics vlan 1
```

Vlan	Forwarded	Dropped	DHCP Drops	ACL Drops
1	0	0	0	0
Vlan	DHCP Permits	ACL Permits	Source MAC Failures	
1	0	0	0	
Vlan	Dest MAC Failures	IP Validation Failures	Invalid Protocol Data	
1	0	0	0	

Related Commands

```
clear ip arp inspection statistics
```

11.11.5 show ip arp inspection vlan

Command Purpose

Use this command to displays the configuration and the operating state of ARP Inspection for the specified vlan.

Command Syntax

```
show ip arp inspection vlan VLAN_RNG_STR
```

Parameter	Parameter Description	Parameter Value
vlan <i>VLAN_RNG_STR</i>	Selected vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

If no vlans are specified or if a range is specified, displays information only for vlans with ARP Inspection enabled.

Examples

This example shows how to display the arp inspection statistics:

```
Switch# show ip arp inspection vlan 1
```

```
Source Mac Validation      : Disabled
```

```
Destination Mac Validation : Disabled
```

```
IP Address Validation      : Disabled
```

Vlan	Configuration	ACL Match	Static ACL

1	enabled	acl	

Vlan	ACL Logging	DHCP Logging

1	deny	deny

Related Commands

```
ip arp inspection vlan
```

11.11.6 show debugging arp inspection

Command Purpose

Use this command to display the debug information of ARP Inspection.

Command Syntax

```
show debugging arp inspection
```

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to display the debug information of ARP Inspection:

```
Switch# show debugging arp inspection
```

```
arp inspection debugging status:
```

```
  packet debugging is on
```

```
  error debugging is on
```

Related Commands

```
debug arp inspection
```

11.11.7 debug arp inspection

Command Purpose

Use this command to configure ARP Inspection debug.

Command Syntax

```
debug arp inspection ( all | packet | events | error )
```

Parameter	Parameter Description	Parameter Value
all	Turn all debugging on	-
packet	ARP message fields	-
events	ARP Inspection events	-
error	Error DHCP message	-

Command Mode

Privileged EXEC

Default

All debug disabled.

Usage

This command is used to debug arp inspection, including all, error, events, packet.

Examples

This example shows how to use this command to debug all error ARP packet:

```
Switch# debug ip arp inspection error
```

Related Commands

```
show debugging arp inspection
```

11.11.8 ip arp inspection filter vlan

Command Purpose

Use this command to applies the ARP ACL to a VLAN.

Command Syntax

ip arp inspection filter acl vlan *VLAN_RNG_STR* (static |)

Parameter	Parameter Description	Parameter Value
acl	ARP acl name	-
VLAN_RNG_STR	Selected vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11
static	Apply the ACL statically	-

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to apply the ARP ACL to a vlan 2:

```
Switch# configure terminal
```

```
Switch(config)# ip arp inspection filter acl vlan 2 static
```

Related Commands

arp access-list

11.11.9 ip arp inspection log-buffer entries

Command Purpose

Use this command to set log-buffer size.

Command Syntax

ip arp inspection log-buffer entries *NUMBER*

Parameter	Parameter Description	Parameter Value
NUMBER	Number of log buffer	10-1024

Command Mode

Global Configuration

Default

None

Usage

The no command reverts the log-buffer to the default buffer size (32).

Examples

This example shows how to set log-buffer size to 10:

```
Switch# configure terminal
```

```
Switch(config)# ip arp inspection log-buffer entries 10
```

Related Commands

show ip arp inspection log

11.11.10 ip arp inspection log-buffer logs interval

Command Purpose

Use this command to configure the DAI logging system messages. The no command reverts the default system message configuration.

Command Syntax

ip arp inspection log-buffer logs *NUMBER* interval *INTERVAL*

no ip arp inspection log-buffer logs

Parameter	Parameter Description	Parameter Value
NUMBER	Number of log buffer	0-1024
INTERVAL	Interval (seconds)	0-86400 seconds

Command Mode

Global Configuration

Default

Default number of log buffer is 5, default interval is 1

Usage

A 0 value for the logs number indicates that the entries should not be logged out of this buffer. The default number is 5.

A 0 value for the interval seconds keyword and argument indicates an immediate log. The default number is 1.

Examples

This example shows how to configure logging to send 12 messages every 2 seconds:

```
Switch# configure terminal
```

```
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
```

Related Commands

None

11.11.11 ip arp inspection validate

Command Purpose

Use this command to enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Command Syntax

[no] ip arp inspection validate (dst-mac | ip | src-mac)

Parameter	Parameter Description	Parameter Value
dst-mac	Validate destination MAC address	-
ip	Validate IP addresses	-
src-mac	Validate source MAC address	-

Command Mode

Global Configuration

Default

No default is defined.

Usage

For src-mac, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For dst-mac, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For ip, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Examples

This example shows how to enable additional validation on the destination MAC address.:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
```

Related Commands

```
show ip arp inspection
```

11.11.12 ip arp inspection vlan

Command Purpose

Use this command to enable ARP Inspection on vlans.

Command Syntax

```
[ no ] ip arp inspection vlan VLAN_ID
```

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11

Command Mode

Global Configuration

Default

No default is defined.

Usage

Enable ARP Inspection on vlans.

Examples

This example shows how to enable ARP Inspection on VLAN 2::

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2
```

Related Commands

show ip arp inspection vlan 2

11.11.13 ip arp inspection vlan logging acl-macth

Command Purpose

Use this command to configure ARP Inspection log filtering.

Command Syntax

[no] ip arp inspection vlan *VLAN_ID* logging acl-macth (matchlog | none)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11
matchlog	Log packets on ACE logging configuration	-
none	Do not log packets that match ACLs	-

Command Mode

Global Configuration

Default

No default is defined.

Usage

If you specify the matchlog keyword in this command and the log keyword in the permit or deny ARP access-list configuration command, ARP packets permitted or denied by the ARP Inspection are logged.

Examples

This example shows how to log permitted ARP packets on vlan 2:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog
```

Related Commands

ip arp inspection vlan

11.11.14 ip arp inspection vlan logging dhcp-bindings

Command Purpose

Use this command to configure ARP Inspection log filtering.

Command Syntax

[no] ip arp inspection vlan *VLAN_ID* logging dhcp-bindings (all | none | permit)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Vlan range	valid vlan ID range is 1-4094. Use short bar(-) to describe continuous VLANs, use comma(,) to describe non-continuous VLANs. For example:1, 3-5, 7, 9-11
all	Log all packets that match DHCP bindings	-
permit	Log DHCP Binding Permitted packets	-
none	Do not log packets that match DHCP bindings	-

Command Mode

Global Configuration

Default

No default is defined.

Usage

If the command is set, the information that match the dhcp-bings will be logged.

Examples

This example shows how to Logs all packets that match DHCP bindings on vlan 2:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 2 logging dhcp-bindings all
```

Related Commands

show ip arp inspection vlan

11.11.15 clear ip arp inspection log-buffer

Command Purpose

Use this command to delete all log in log-buffer.

Command Syntax

clear ip arp inspection log-buffer

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to delete all log in log-buffer.

Examples

This example shows how to delete all log in log-buffer:

```
Switch# clear ip arp inspection log-buffer
```

Related Commands

ip arp inspection log-buffer logs

11.11.16 clear ip arp inspection statistics

Command Purpose

Use this command to delete all statistics of ARP Inspection.

Command Syntax

```
clear ip arp inspection statistics
```

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to delete all statistics of ARP Inspection.

Examples

This example shows how to delete all statistics of ARP Inspection:

```
Switch(config)# clear ip arp inspection statistics
```

Related Commands

```
show ip arp inspection statistics
```

11.11.17 ip arp inspection trust

Command Purpose

Use this command to configure the ARP Inspection interface trust state.

Command Syntax

```
ip arp inspection trust  
no ip arp inspection trust
```

Command Mode

Interface Configuration

Default

No default is defined.

Usage

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted.

Examples

This example shows how to configure the ARP Inspection interface eth-0-2 untrusted state:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# no ip arp inspection trust
```

Related Commands

show ip arp inspection interfaces

11.11.18 arp access-list

Command Purpose

Use this command to configure a ARP ACL

Command Syntax

```
arp access-list ACL_NAME
no arp access-list ACL_NAME
```

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	A arp access-list name	String with up to 40 characters

Command Mode

Global Configuration

Default

No default is defined.

Usage

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

Examples

This example shows how to configure a ARP ACL:

```
Switch# configure terminal
Switch(config)# arp access-list acl1
```

Related Commands

show access-list arp

11.11.19 ip mac

Command Purpose

Use this command to configure ARP ACEs.

Command Syntax

(deny | permit) (request | response |) ip (IP_ADDR IP_ADDR_MASK | any | host IP_ADDR) mac (MAC_ADDR MAC_ADDR_MASK | any | host MAC_ADDR) (log |)

Parameter	Parameter Description	Parameter Value
deny	Specify packets to reject	-
permit	Log all packets that match DHCP bindings	-
request	Log DHCP Binding Permitted packets	-
response	Do not log packets that match DHCP bindings	-
IP_ADDR	Sender address	IPv4 address
IP_ADDR_MASK	Sender wildcard bits	IPv4 wildcard
any	Any sender host	-
host	A single Sender host	-
MAC_ADDR	Sender host's MAC address	MAC address in HHHH.HHHH.HHHH format
MAC_ADDR_MASK	Sender wildcard	MAC wildcard in HHHH.HHHH.HHHH format
log	Log at match	-

Command Mode

ARP ACL Configuration

Default

No default is defined.

Usage

Use this command to add ARP ACE to ARP ACL.

Examples

This example shows how to configure a ARP ACE:

```
Switch# configure terminal
Switch(config)# arp access-list acl1
Switch(config-arp-acl)# permit ip host 192.168.1.1 mac any
```

Related Commands

show access-list arp

11.11.20 no sequence-num

Command Purpose

Use this command to delete a ARP ACE.

Command Syntax

no sequence-num *NUMBER*

Parameter	Parameter Description	Parameter Value
NUMBER	Specify a sequence number	1-131071

Command Mode

ARP ACL Configuration

Default

No default is defined.

Usage

This command is used to delete ARP ACE configured.

Examples

This example shows how to delete a ARP ACE:

```
Switch# configure terminal
Switch(config)# arp access-list acl1
Switch(config-arp-acl)# no sequence-num 10
```

Related Commands

show access-list arp

11.11.21 show access-list arp

Command Purpose

Use this command to display the arp acl configuration.

Command Syntax

show access-list arp (*ACL_NAME* |)

Parameter	Parameter Description	Parameter Value
<i>ACL_NAME</i>	A arp access-list name	String with up to 40 characters

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to display the arp acl configured by arp acl.

Examples

This example shows how to display arp ace:

```
Switch# show access-list arp
```

```
arp access-list acl
```

```
10 permit request ip 1.1.1.1 0.255.255.255 mac any
```

Related Commands

arp access-list

11.12 DHCP Snooping Commands

11.12.1 clear dhcp snooping

Command Purpose

Use the clear dhcp snooping global configuration command on the switch to clear dynamic entries in DHCP binding database or the DHCP snooping statistics counters.

Command Syntax

clear dhcp snooping (bindings (learning | manual) (ipv4 *IP_ADDR* | mac *MAC_ADDR* | vlan *VLAN_ID* | interface *IFNAME* |) | statistics)

Parameter	Parameter Description	Parameter Value
bindings	Clear the DHCP snooping binding database	-
IP_ADDR	Clear the binding entry by IP address	IPv4 Address
MAC_ADDR	Clear the binding entry by MAC address	MAC Address
VLAN_ID	Clear the binding entry by VLAN	1-4094
IFNAME	Clear the binding entry by interface	Support physical and AGG interfaces
statistics	Clear the DHCP snooping statistics counter	-

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to clear DHCP snooping binding or statistics.

Examples

This example shows how to clear the DHCP snooping statistics counters:

```
Switch(config)# clear dhcp snooping statistics
```

Related Commands

show dhcp snooping binding

show dhcp snooping statistics

11.12.2 dhcp snooping

Command Purpose

Use the dhcp snooping global configuration command on the switch to globally enable DHCP snooping. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping

no dhcp snooping

Command Mode

Global Configuration

Default

DHCP snooping is disabled.

Usage

For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping. DHCP snooping is not active until you enable snooping on a VLAN by using the dhcp snooping vlan vlan-id global configuration command.

Examples

This example shows how to enable DHCP snooping:

```
Switch# configure terminal
```

```
Switch(config)# dhcp snooping
```

You can verify your settings by entering the show dhcp snooping config privileged EXEC command:

Related Commands

dhcp snooping vlan

show dhcp snooping config

11.12.3 dhcp snooping binding

Command Purpose

Use the dhcp snooping binding global configuration command on the switch to configure the DHCP snooping binding database and to add binding entries to the database.

Command Syntax

dhcp snooping binding mac *MAC_ADDR* vlan *VLAN_ID* ipv4 *IP_ADDR* interface *IFNAME* expiry *SECONDS*

no dhcp snooping bindings (ipv4 *IP_ADDR* | mac *MAC_ADDR* | vlan *VLAN_ID* | interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Specify a MAC address	MAC Address
VLAN_ID	Specify a VLAN number.	1-4094
IP_ADDR	Specify an IP address	IPv4 Address
IFNAME	Specify an interface on which to add or delete a binding entry	Support physical and AGG interfaces
expiry SECONDS	Specify the interval (in seconds) after which the binding entry is no longer valid.	0 - 86400

Command Mode

Global Configuration

Default

No default database is defined.

Usage

Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the show dhcp snooping binding privileged EXEC command to display the configured bindings.

Examples

This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# configure terminal
```

```
Switch(config)# dhcp snooping binding mac 0001.000c.01ef vlan 1 ipv4 10.10.1.1 interface eth-0-1 expiry 1000
```

Related Commands

dhcp snooping

show dhcp snooping binding

11.12.4 dhcp snooping database

Command Purpose

Use the dhcp snooping database global configuration command on the switch to configure the DHCP snooping binding database agent.

Use the no form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

Command Syntax

dhcp snooping database auto-save interval *SECONDS*

Parameter	Parameter Description	Parameter Value
interval SECONDS	Specify the interval (in seconds) that how long to save the binding database.	15 - 1200 seconds

Command Mode

Global Configuration

Default

Default interval is 600 seconds.

Usage

The DHCP snooping database is save as flash:/dhcpsnooping.

Examples

The following is sample output from the dhcp snooping database command:

```
Switch# configure terminal
Switch(config)# dhcp snooping database auto-save interval 120
```

Related Commands

dhcp snooping
dhcp snooping binding

11.12.5 dhcp snooping information option

Command Purpose

Use the dhcp snooping information option global configuration command on the switch to enable DHCP option-82 data insertion. Use the no form of this command to disable DHCP option-82 data insertion.

Command Syntax

dhcp snooping information option
no dhcp snooping information option

Command Mode

Global Configuration

Default

DHCP option-82 data is not inserted.

Usage

You must globally enable DHCP snooping by using the `dhcp snooping global configuration` command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, `vlan-mod-port`, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts send the reply to the switch if the request has been relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

Examples

This example shows how to enable DHCP option-82 data insertion:

```
Switch# configure terminal
```

```
Switch(config)# dhcp snooping information option
```

You can verify your settings by entering the `show dhcp snooping config` privileged EXEC command.:

```
Switch# show dhcp snooping config
```

```
dhcp snooping service: enabled
```

```
dhcp snooping switch: enabled
```

```
Verification of hwaddr field: enabled
```

```
Insertion of relay agent information (option 82): enabled
```

```
Relay agent information (option 82) on untrusted port: not allowed
```

```
dhcp snooping vlan 1
```

Related Commands

```
show dhcp snooping config
```

```
show dhcp snooping binding
```

11.12.6 dhcp snooping information option allow-untrusted

Command Purpose

Use the dhcp snooping information option allow-untrusted global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the no form of this command to return to the default setting.

Command Syntax

```
dhcp snooping information option allow-untrusted
no dhcp snooping information option allow-untrusted
```

Command Mode

Global Configuration

Default

The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

Usage

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the dhcp snooping information option allow-untrusted command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

Examples

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch# configure terminal
Switch(config)# dhcp snooping information option allow-untrusted
```

Related Commands

```
show dhcp snooping config
```

11.12.7 dhcp snooping information option allow-untrusted (interface)

Command Purpose

Use the dhcp snooping information option allow-untrusted interface configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping information option allow-untrusted
no dhcp snooping information option allow-untrusted

Command Mode

Interface Configuration

Default

Allow-untrusted is not configured on interface. DHCP packets with Option-82 will be processed according to global configuration.

Usage

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the dhcp snooping information option allow-untrusted command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

Examples

This example shows how to configure an interface to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp snooping information option allow-untrusted
```

Related Commands

show dhcp snooping config

11.12.8 dhcp snooping trust

Command Purpose

Use the dhcp snooping trust interface configuration command on the switch to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping trust
no dhcp snooping trust

Command Mode

Interface Configuration

Default

DHCP snooping trust is disabled.

Usage

Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

Examples

This example shows how to enable DHCP snooping trust on a port:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp snooping trust
```

Related Commands

show dhcp snooping config

11.12.9 dhcp snooping verify

Command Purpose

Use the dhcp snooping verify global configuration command on the switch to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the no form of this command to configure the switch to not verify the MAC addresses.

Command Syntax

```
dhcp snooping verify mac-address  
no dhcp snooping verify mac-address
```

Command Mode

Global Configuration

Default

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

Usage

In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

Examples

This example shows how to disable the MAC address verification:

```
Switch# configure terminal  
Switch(config)# no dhcp snooping verify mac-address
```

Related Commands

```
show dhcp snooping config
```

11.12.10 dhcp snooping vlan

Command Purpose

Use the dhcp snooping vlan global configuration command on the switch to enable DHCP snooping on a VLAN. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping vlan *VLAN-RANGE*

no dhcp snooping vlan *VLAN-RANGE*

Parameter	Parameter Description	Parameter Value
VLAN-RANGE	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping.	1-4094

Command Mode

Global Configuration

Default

DHCP snooping is disabled on all VLANs.

Usage

You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch# configure terminal
```

```
Switch(config)# dhcp snooping vlan 10
```

Related Commands

```
show dhcp snooping config
```

11.12.11 dhcp snooping vlan information option format-type circuit-id string

Command Purpose

Use this interface configuration command on the switch stack or on a standalone switch to configure the option-82 circuit-ID suboption. Use the no form of this command to configure the default circuit-ID suboption.

Command Syntax

dhcp snooping vlan *VLAN_ID* information option format-type circuit-id string *STRING*

no dhcp snooping vlan *VLAN_ID* information option format-type circuit-id string

Parameter	Parameter Description	Parameter Value
VLAN_ID	Specify a VLAN ID.	1-4094

Parameter	Parameter Description	Parameter Value
STRING	ASCII string for circuit id	ASCII string with up to 63 characters

Command Mode

Interface Configuration

Default

None

Usage

User must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples

This example shows how configure the option-82 circuit-ID suboption:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# dhcp snooping vlan 2 information option format-type circuit-id string vlan2
```

Related Commands

None

11.12.12 dhcp snooping information option format remote-id**Command Purpose**

Use the dhcp snooping information option format remote-id global configuration command on the switch stack or on a standalone switch to configure the option-82 remote-ID suboption. Use the no form of this command to configure the default remote-ID suboption.

Command Syntax

dhcp snooping information option format remote-id (string *NAME* | hostname)

no dhcp snooping information option format remote-id

Parameter	Parameter Description	Parameter Value
NAME	Specify a remote ID	ASCII string with up to 63 characters(no spaces)
hostname	Specify the switch hostname as the remote ID	-

Command Mode

Global Configuration

Default

None

Usage

You must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples

This example shows how configure the option-82 remote-ID suboption:

```
Switch# configure terminal
```

```
Switch(config)# dhcp snooping information option format remote-id hostname
```

Related Commands

None

11.12.13 debug dhcp snooping**Command Purpose**

Use this command to turn on the debug switches of dhcp snooping module.

To restore the default, use the no form of this command

Command Syntax

debug dhcp snooping (events | error | dump | packet | all)

no debug dhcp snooping (events | error | dump | packet | all)

Parameter	Parameter Description	Parameter Value
events	Snooping events	-
error	Error DHCP message	-
packet	DHCP message fields	-
dump	Dump message in hex format	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.

Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcp snooping debug switches:

```
Switch# debug dhcp snooping all
```

Related Commands

terminal monitor

show logging buffer

11.12.14 show dhcp snooping binding

Command Purpose

Use the show dhcp snooping binding privileged EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

Command Syntax

show dhcp snooping binding ((all | manual | learning) (ipv4 *IP_ADDR* | mac *MAC_ADDR* | vlan *VLAN_ID* | interface *IFNAME* |) summary | database)

Parameter	Parameter Description	Parameter Value
all	Display all entries	-
manual	Display static entries	-
learning	Display dynamic entries	-
MAC_ADDR	Specify MAC address	MAC Address
VLAN_ID	Specify a VLAN number.	1-4094
IP_ADDR	Specify an IP address	IPv4 Address
IFNAME	Specify an interface on which to add or delete a binding entry	Support physical and aggregation interfaces
summary	Display summary information of DHCP snooping bindings	-
database	Display stored information of DHCP snooping bindings	-

Command Mode

Privileged EXEC

Default

None

Usage

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Examples

The following is sample output from the show dhcp snooping binding command:

```
Switch# show dhcp snooping binding all
```

DHCP snooping binding table:

VLAN	MAC Address	Interface	Lease(s)	IP Address

1	0001.0001.0001	eth-0-2	static	1.1.1.1

Related Commands

dhcp snooping binding

11.12.15 show dhcp snooping config**Command Purpose**

Use the show dhcp snooping privileged EXEC command to display the DHCP snooping configuration.

Command Syntax

```
show dhcp snooping config
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping config command:

```
Switch# show dhcp snooping config
```

```
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): enabled
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 1
```

Related Commands

dhcp snooping binding

11.12.16 show dhcp snooping statistics

Command Purpose

Use the show dhcp snooping statistics privileged EXEC command to display DHCP snooping statistics.

Command Syntax

```
show dhcp snooping statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the statistics of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping statistics command:

```
Switch# show dhcp snooping statistics
```

```
DHCP snooping statistics:
```

```
=====
DHCP packets                               11257
```

BOOTP packets	0
Packets forwarded	10381
Packets invalid	844
Packets MAC address verify failed	354
Packets dropped	516

Related Commands

clear dhcp snooping statistics

11.12.17 show dhcp snooping trusted-sources

Command Purpose

Use the show dhcp snooping trusted-sources command to display DHCP snooping trusted interfaces.

Command Syntax

show dhcp snooping trusted-sources

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the trusted interfaces of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping trusted-sources command:

```
Switch# show dhcp snooping trusted-sources
```

```
List of DHCP snooping trusted interface(s):
```

```
=====
```

```
eth-0-2
```

Related Commands

dhcp snooping trust

11.13 IP Source Guard Commands

11.13.1 ip source binding

Command Purpose

Use the ip source binding global configuration command on the switch to configure static IP source bindings on the switch. Use the no form of this command to delete static bindings.

Command Syntax

ip source binding mac *MAC_ADDR* vlan *VLAN_ID* ip *IP_ADDR* interface *IFNAME*

no ip source binding mac *MAC_ADDR* vlan *VLAN_ID* ip *IP_ADDR* interface *IFNAME*

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Specify a MAC address	MAC Address
VLAN_ID	Specify a VLAN number	1-4094
IP_ADDR	Specify an IPv4 address	IPv4 Address
IFNAME	Specify an interface on which to add or delete a binding entry	Support physical and aggregation interfaces

Command Mode

Global Configuration

Default

None

Usage

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number.

The same MAC and IP can only be bound in one binding entry. Duplication of MAC or IP in binding entries is not allowed.

No IP source bindings are configured by default.

Examples

The following is sample output from the ip source binding command:

```
Switch# configure terminal
```

```
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ip 172.20.50.5 interface eth-0-1
```

Related Commands

show ip source binding

no ip source binding

11.13.2 ipv6 source binding

Command Purpose

Use the ip source binding global configuration command on the switch to configure static IP source bindings on the switch. Use the no form of this command to delete static bindings.

Command Syntax

ip source binding mac *MAC_ADDR* vlan *VLAN_ID* ipv6 *IPv6_ADDR* interface *IFNAME*

no ip source binding mac *MAC_ADDR* vlan *VLAN_ID* ipv6 *IPv6_ADDR* interface *IFNAME*

Parameter	Parameter Description	Parameter Value
MAC_ADDR	Specify a MAC address	MAC Address
VLAN_ID	Specify a VLAN number	1-4094
IPv6_ADDR	Specify an IPv6 address	IPv6 Address
IFNAME	Specify an interface on which to add or delete a binding entry	Support physical and aggregation interfaces

Command Mode

Global Configuration

Default

None

Usage

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number.

The same MAC and IP can only be bound in one binding entry. Duplication of MAC or IP in binding entries is not allowed.

No IP source bindings are configured by default.

Examples

The following is sample output from the ip source binding command:

```
Switch# configure terminal
```

```
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ipv6 1::12:11 interface eth-0-1
```

Related Commands

show ip source binding

no ip source binding

11.13.3 no ip source binding entries

Command Purpose

Use this command to delete one or more ip source binding entries.

Command Syntax

no ip source binding entries

no ip source binding entries vlan *VLAN_ID*

no ip source binding entries interface *IFNAME*

Parameter	Parameter Description	Parameter Value
VLAN_ID	Specify a VLAN number	1-4094
IFNAME	Specify an interface on which to add or delete a binding entry	Support physical and aggregation interfaces

Command Mode

Global Configuration

Default

None

Usage

If neither vlan-id nor interface-id is specified, all static ip source binding entries will be deleted.

Examples

clear the entries of eth-0-1:

```
Switch# configure terminal
```

```
Switch(config)# no ip source binding entries interface eth-0-1
```

clear the entries of vlan2:

```
Switch# configure terminal
```

```
Switch(config)# no ip source binding entries vlan 2
```

Related Commands

ip source binding

show ip source binding

11.14 AAA Commands

11.14.1 aaa new-model

Command Purpose

Use this command to enable the authentication, authorization, accounting (AAA) access control model.

Use the no form of this command to disable AAA model

Command Syntax

```
aaa new-model
```

```
no aaa new-model
```

Command Mode

Global Configuration

Default

None

Usage

Enables the AAA access control model

Examples

The following example shows how to enable AAA access control model:

```
Switch# configure terminal
```

```
Switch(config)# aaa new-model
```

Related Commands

```
show aaa status
```

11.14.2 aaa authentication login

Command Purpose

Use this command to set authentication, authorization, accounting (AAA) authentication at login.

Use the no form of this command to disable authentication at login

Command Syntax

aaa authentication login (default | *LISTNAME*) { enable | line | none | radius | local | tacacs-plus }

no aaa authentication login (default | *LISTNAME*)

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An authentication list with this name	String with up to 31 characters
enable	Enable password	-
line	Line password	-
none	No authentication	-
radius	RADIUS server	-
local	Local username	-
tacacs-plus	TACACS+	-

Command Mode

Global Configuration

Default

None

Usage

Use the aaa authentication login global configuration command to specify one or more AAA methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set authentication at login:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default local radius none
```

Related Commands

show aaa method-lists authentication

11.14.3 aaa authorization exec

Command Purpose

Set authentication, authorization, accounting (AAA) authorization at login.

Command Syntax

aaa authorization exec (default | *LISTNAME*) { none | radius | local | tacacs-plus }

no aaa authorization exec (default | *LISTNAME*)

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An authentication list with this name	String with up to 31 characters
none	No authentication	-
radius	RADIUS server	-
local	Local username	-
tacacs-plus	TACACS+	-

Command Mode

Global Configuration

Default

None

Usage

Use the aaa authorization exec global configuration command to specify one or more AAA authorization methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set authorization at login:

```
Switch# configure terminal
```

```
Switch(config)# aaa new-model
```

```
Switch(config)# aaa authorization exec default local radius none
```

Related Commands

None

11.14.4 aaa accounting exec

Command Purpose

Set authentication, authorization, accounting (AAA) accounting at login.

Command Syntax

aaa accounting exec (default | *LISTNAME*) (((start-stop | stop-only) { radius | tacacs-plus } { none | }) | none)

no aaa accounting exec (default | *LISTNAME*)

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An accounting list with this name	String with up to 31 characters
start-stop	Send exec accounting start and stop request while logging switch	-
stop-only	Only send exec accounting stop request while exit switch	-
none	No accounting	-
radius	RADIUS server	-
tacacs-plus	TACACS+	-

Command Mode

Global Configuration

Default

None

Usage

Use the aaa accounting exec global configuration command to specify one or more AAA accounting methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set accounting exec:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa accounting exec default start-stop tacacs-plus none
```

Related Commands

None

11.14.5 aaa accounting commands

Command Purpose

Set authentication, authorization, accounting (AAA) accounting at login.

Command Syntax

aaa accounting commands (default | *LISTNAME*) ((tacacs-plus (none |)) | none)

no aaa accounting commands (default | *LISTNAME*)

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An accounting list with this name	String with up to 32 characters
none	No accounting	-
tacacs-plus	TACACS+	-

Command Mode

Global Configuration

Default

None

Usage

Use the aaa accounting commands global configuration command to specify one or more AAA accounting methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set accounting commands:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa accounting commands default tacacs-plus none
```

Related Commands

None

11.14.6 aaa privilege mapping

Command Purpose

Set the mapping range in AAA server and switch.

Command Syntax

aaa privilege mapping *LEVEL1 LEVEL2 LEVEL3*

no aaa privilege mapping

Parameter	Parameter Description	Parameter Value
LEVEL1	The max server privilege mapping to switch level 1, default 0	0-12
LEVEL2	The max server privilege mapping to switch level 2, default 1	1-13
LEVEL3	The max server privilege mapping to switch level 3, default 10	2-14

Command Mode

Global Configuration

Default

0: The server privilege 0 mapping to switch level 1
1: The server privilege 1 mapping to switch level 2
9: The server privilege 2~9 mapping to switch level 3
Other: The server privilege 10~15 mapping to switch level 4

Usage

Use the aaa privilege mapping global configuration command to set the mapping range in AAA server and switch.

Examples

The following example shows how to set accounting commands:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa privilege mapping 0 1 14
```

Related Commands

None

11.14.7 login authentication

Command Purpose

Enable authentication, authorization, accounting (AAA) authentication for logins.

Command Syntax

login authentication (default | *LISTNAME*)

no login authentication

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An authentication list with this name	String with up to 31 characters

Command Mode

Line Configuration

Default

None

Usage

None

Examples

The following example shows how to enable authentication for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# login authentication default
```

Related Commands

show aaa method-lists authentication

11.14.8 authorization exec

Command Purpose

Enable authentication, authorization, accounting (AAA) authorization for logins.

Command Syntax

authorization exec (default | *LISTNAME*)

no authorization exec

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An authorization list with this name	String with up to 31 characters

Command Mode

Line Configuration

Default

None

Usage

None

Examples

The following example shows how to enable authorization for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# authorization exec default
```

Related Commands

None

11.14.9 accounting exec**Command Purpose**

Enable authentication, authorization, accounting (AAA) accounting for logins.

Command Syntax

accounting exec (default | *LISTNAME*)

no accounting exec

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An accounting list with this name	String with up to 31 characters

Command Mode

Line Configuration

Default

None

Usage

None

Examples

The following example shows how to enable accounting for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting exec default
```

Related Commands

None

11.14.10 accounting commands

Command Purpose

Enable authentication, authorization, accounting (AAA) accounting for logins.

Command Syntax

accounting commands (default *LISTNAME*)

no accounting commands

Parameter	Parameter Description	Parameter Value
default	Default method list	-
LISTNAME	An accounting list with this name	String with up to 31 characters

Command Mode

Line Configuration

Default

None

Usage

None

Examples

The following example shows how to enable accounting for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting commands default
```

Related Commands

None

11.14.11 show aaa method-lists authentication

Command Purpose

Use this command to show authentication, authorization, accounting (AAA) authentication method lists.

Command Syntax

```
show aaa method-lists authentication
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show authentication, authorization, accounting (AAA) authentication method lists.

Examples

The following example shows how to show authentication method lists:

```
Switch# show aaa method-lists authentication
```

```
authen queue = AAA_ML_AUTHEN_LOGIN
  name = default  state = ALIVE :   radius
authen queue = AAA_ML_AUTHEN_LOGIN
  name = group_a  state = ALIVE :   radius  local  line  enable  none
authen queue=AAA_ML_AUTHEN_LOGIN
  name = group_b  state = ALIVE :   local  line  none
```

Related Commands

aaa authentication login

11.14.12 show aaa status

Command Purpose

Use this command to show authentication, authorization, accounting (AAA) status.

Command Syntax

```
show aaa status
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show authentication, authorization, accounting (AAA) status.

Examples

The following example shows how to show authentication, authorization, accounting status:

```
Switch# show aaa status
```

```
aaa stats:
```

```
    Authentication enable
```

Related Commands

```
aaa new-model
```

11.14.13 show aaa privilege mapping

Command Purpose

Use this command to show privilege mapping relationship with server privilege.

Command Syntax

```
show aaa privilege mapping
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is to show privilege mapping relationship with server privilege.

Examples

The following example shows how to show authentication method lists:

```
Switch# show aaa privilege mapping
```

Server	Switch	Server
=====		
0	1	0
1	2	1
2~10	3	10
11~15	4	15

Related Commands

aaa privilege mapping

11. 15 RADIUS Authentication Commands

11.15.1 radius-server deadtime

Command Purpose

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the radius-server deadtime command in global configuration mode. To set dead-time to default value, use the no form of this command.

Command Syntax

radius-server deadtime *MINUTES*

no radius-server deadtime

Parameter	Parameter Description	Parameter Value
MINUTES	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests	1-20 minutes

Command Mode

Global Configuration

Default

5 minutes

Usage

Use this command to cause the switch to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as "dead" is skipped by additional requests for the duration of minutes, unless there are no servers not marked "dead".

The default value of the radius deadtime is 5 minutes.

Examples

The following is sample output from the radius deadtime command:

```
Switch# configure terminal
Switch(config)# radius deadtime 10
```

Related Commands

radius-server host

11.15.2 radius-server host

Command Purpose

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

Command Syntax

```
radius-server host HOST_IP_ADDR ( source-interface IFNAME | source-ip SRC_IP_ADDR | )
radius-server host HOST_IP_ADDR { key ( 8 | secret | ) STRING | retransmit RETRIES | timeout SEC | mgmt-if IPV4_ADDR auth-port AUTH_PORT }
( source-interface IFNAME | source-ip SRC_IP_ADDR | )
radius-server host mgmt-if IPV4_ADDR
```



```
radius-server host mgmt-if IPV4_ADDR { key ( 8 | secret | ) STRING | retransmit RETRIES | timeout SEC | mgmt-if IPV4_ADDRauth-port AUTH_PORT }
```

```
no radius-server host ( mgmt-if | ) IPV4_ADDR ( mgmt-if IPV4_ADDRauth-port AUTH_PORT | )
```

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
IPV4_ADDR	IPv4 address of the RADIUS server host	IPv4 Address
IPV6_ADDR	IPv6 address of the RADIUS server host	-
AUTH_PORT	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1812	1-65535
SECONDS	(Optional) Specifies the timeout value.If no timeout value is specified, the global value is used. The default value should be 5	1-1000 seconds
RETRIES	(Optional) Specifies the retransmit value. If no retransmit value is specified, the global value is used. The default value should be 3	1-100
STRING	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. This key must match the encryption used on the RADIUS daemon	Up to 256 characters
IFNAME	Name of source interface	Support physical/aggregation /loopback/vlan/tunnel ports
SRC_IP_ADDR	Source IP address	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

The following is sample output from the radius-server host command:

```
Switch# configure terminal
Switch(config)# radius-server host 10.10.1.1 key abcde
```

Related Commands

radius-server key

radius-server timeout

11.15.3 radius-server retransmit

Command Purpose

To specify the number of times the switch searches the list of RADIUS server hosts before giving up, use the radius-server retransmit command in global configuration mode. To disable retransmission, use the no form of this command.

Command Syntax

radius-server retransmit *RETRIES*

no radius-server retransmit

Parameter	Parameter Description	Parameter Value
RETRIES	Maximum number of retransmission attempts. The default is 3	1-100

Command Mode

Global Configuration

Default

3 attempts

Usage

The switch tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the switch, we recommend that you configure the RADIUS server retransmit rate to 5. The default value of radius retransmit is 3 attempts.

Examples

The following is sample output from the radius retransmit command:

```
Switch# configure terminal
Switch(config)# radius retransmit 5
```

Related Commands

radius-server host

radius-server key

11.15.4 radius-server timeout

Command Purpose

To set the interval for which a switch waits for a server host to reply, use the radius-server timeout command in global configuration mode. To restore the default, use the no form of this command.

Command Syntax

radius-server timeout *SECONDS*

no radius-server timeout

Parameter	Parameter Description	Parameter Value
SECONDS	Number that specifies the timeout interval, in seconds. The default is 5 seconds.	1-1000 seconds

Command Mode

Global Configuration

Default

None

Usage

Use this command to set the number of seconds a switch waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the switch, we recommend that you configure the RADIUS server timeout to 15 seconds.

The default value of radius timeout is 5 seconds.

Examples

The following is sample output from the radius timeout command:

```
Switch# configure terminal
Switch(config)# radius retransmit 15
```

Related Commands

radius-server host
radius-server key

11.15.5 radius-server key

Command Purpose

To set the shared encryption key of RADIUS server, use the radius-server key command in global configuration mode. To restore the default, use the no form of this command.

Command Syntax

radius-server key *KEY_STRING*
no radius-server key

Parameter	Parameter Description	Parameter Value
KEY_STRING	RADIUS server key-string	-

Command Mode

Global Configuration

Default

None

Usage

Use this command to set the shared encryption key in a switch.

Shared encryption key is the foundation of communicate between switch and server. You need set a same shared encryption string in authentication server and switch.

Examples

The following is sample output from the radius-server key command:

```
Switch# configure terminal
Switch(config)# radius-server key simple-key
```

Related Commands

radius-server host

11.15.6 show dot1x radius-server status

Command Purpose

Use the "show radius-server" command to display radius server states of each IEEE 802.1x session.

Command Syntax

show dot1x radius-server status (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
IFNAME	Specify an interface to show	Support Physical ports

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the current radius-server and dead radius-servers of each IEEE 802.1 x sessions.

Examples

The following is sample output from the show radius-server command:

```
Switch# show dot1x radius-server status
```

```
=====
802.1X session on interface eth-0-9:
current radius server:
  retransmit count   : 3
  server address     : 3.3.3.3:1812
  socket descriptor  : 15
  last state         :
radius servers in dead list:
  N/A
=====
```

Related Commands

radius-server host

11.15.7 show radius-server

Command Purpose

Use the "show radius-server" command to display radius server states of each IEEE 802.1x session.

Command Syntax

show radius-server

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the current radius-server and dead radius-servers of each IEEE 802.1 x sessions.

Examples

The following is sample output from the show radius-server command:

```
Switch# show radius-server
```

```
=====
802.1X session on interface eth-0-9:
current radius server:
  retransmit count   : 3
  server address     : 3.3.3.3:1812
  socket descriptor  : 15
  last state         :
radius servers in dead list:
  N/A
=====
```

Related Commands

radius-server host

11. 16 Tacacs+ Commands

11.16.1 tacacs-server host

Command Purpose

Specifies and defines the IP address of the TACACS+ server host.

Command Syntax

```
tacacs-server host HOST_IP_ADDR ( { key ( 8 | secret | ) STRING | timeout SECONDS | port PORT | single-connection } | ) ( source-interface IFNAME | source-ip SRC_IP_ADDR | )
```

```
tacacs-server host mgmt-if IP_ADDR ( { key ( 8 | secret | ) STRING | timeout SECONDS | port PORT | single-connection } | )
```

```
no tacacs-server host ( mgmt-if | ) IP_ADDR ( port PORT | )
```

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
IP_ADDR	TACACS+ server IP address	IPv4 address
single-connection	Maintains a single open connection	-
PORT	TACACS server port number (default 49)	1-65535
SECONDS	Time to wait for a TACACS server to reply, the range is 1 to 20, default 5s	1-20
STRING	Set TACACS+ encryption key	Up to 256 characters
8	Specifies a hidden password will follow	-
secret	Display the current shared key with cipher text	-
IFNAME	Name of source interface	Support physical/aggregation/loopback/vlan/tunnel ports
SRC_IP_ADDR	Source IP address	IPv4 address

Command Mode

Global Configuration

Default

No Tacacs+ server is configured by default

Usage

Add or delete a TACACS+ server host.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

The following example shows how to specify a TACACS+ server host:

```
Switch# configure terminal
Switch(config)# tacacs-server host 10.10.10.1 port 55 key my_key
```

Related Commands

show tacacs

11.16.2 clear tacacs statistics

Command Purpose

To reset statistics on TACACS+ servers, use the clear tacacs statistics EXEC command.

Command Syntax

clear tacacs statistics

Command Mode

Privileged EXEC

Default

None

Usage

Reset statistics on TACACS+ servers.

Examples

The following example shows how to reset statistics on TACACS+ servers:

```
Switch# clear tacacs statistics
```

Related Commands

show tacacs

11.16.3 show tacacs

Command Purpose

To display statistics for a TACACS+ server, use the show tacacs command in EXEC configuration mode.

Command Syntax

```
show tacacs
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show TACACS+ servers statistics.

Examples

The following example shows how to show TACACS+ servers:

```
Switch(config)# clear tacacs statistics
```

```
Switch# show tacacs
```

```
Tacacs+ Server      : 1.2.3.4/49
      Socket opens:      1
      Socket closes:    0
      Socket aborts:    0
      Socket errors:    0
      Socket Timeouts:  0
      Failed Connect Attempts: 0
      Total Packets Sent: 2
      Total Packets Recv: 2
```

Related Commands

```
tacacs-server host
```

11. 17 Port Isolate Commands

11.17.1 port-isolate group

Command Purpose

Use the port-isolate group interface configuration command on the switch to set the isolate group of a interface.

Use the no form of this command to return to the default setting.

Command Syntax

port-isolate group *GROUP*

no port-isolate group

Parameter	Parameter Description	Parameter Value
GROUP	Port isolate group id	1-30

Command Mode

Interface Configuration

Default

None

Usage

The ports in the same isolate-group can not communicate with each other.

The ports in different isolate-groups should not be affected by this feature.

The isolate-groups can only be configured on physical port and Link Aggregation.

Examples

The following is sample output from the port-isolate group command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# port-isolate group 4
```

Related Commands

port-isolate mode

11.17.2 port-isolate mode

Command Purpose

Use the port-isolate mode global configuration command on the switch to set isolate mode.

Use the no form of this command to return to the default setting.

Command Syntax

port-isolate mode (all | l2)

no port-isolate mode

Parameter	Parameter Description	Parameter Value
all	Isolate bridged packets and routed packets	-

Parameter	Parameter Description	Parameter Value
I2	Isolate bridged packets	-

Command Mode

Global Configuration

Default

None

Usage

If configure "port-isolate mode I2", all routed packets should not obey the port isolate rules.

If configure "port-isolate mode all", all packets should obey the port isolate rules.

The default setting is "I2"

Examples

The following is sample output from the port-isolate mode command:

```
Switch# configure terminal
```

```
Switch(config)# port-isolate mode all
```

Related Commands

port-isolate group

11.17.3 show port-isolate**Command Purpose**

Use the show port-isolate command on the switch to check the port-isolate configuration.

Command Syntax

show port-isolate (group *GROUP*)

Parameter	Parameter Description	Parameter Value
GROUP	Port isolate group id	1-30

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following is sample output from the show port-isolate command:

```
switch # show port-isolate group 12
```

```
Port Isolate Mode   : L2
```

```
-----  
Port Isolate Groups:
```

```
-----  
Groups ID: 12
```

```
eth-0-1  eth-0-2  eth-0-3  eth-0-4  eth-0-5
```

```
eth-0-6  
-----
```

Related Commands

port-isolate group

11.17.4 port-isolate am

Command Purpose

Use this command to enable unidirectional isolation.

Use the no form of this command to disable it.

Command Syntax

port-isolate am interface IFNAME

port-isolate am interface range IFRNG

no port-isolate am interface IFNAME

no port-isolate am interface range IFRNG

no port-isolate am

Parameter	Parameter Description	Parameter Value
IFNAME	port name	Support physical/aggregation ports
IFRNG	string to defining port range	Support physical/aggregation ports. Use comma and short bar to describe a range of ports.

Command Mode

Interface Configuration

Default

None

Usage

Unidirectional isolation can not co-work with isolate group on a same interface.

Examples

The following example shows how to deny the packet received from eth-0-9 and send to eth-0-10:

```
Switch# configure terminal
```

```
Switch(config)# interface eth-0-9
```

```
Switch(config-if)# port-isolate am interface eth-0-10
```

Related Commands

show port-isolate

11. 18 Private Vlan Commands

11.18.1 switchport mode private-vlan

Command Purpose

To configure the switch port's mode as private vlan, use the "switchport mode private-vlan" command in interface mode.

Command Syntax

switchport mode private-vlan (host | promiscuous)

Parameter	Parameter Description	Parameter Value
host	Set the port as private vlan, host port	-
promiscuous	Set the port as private vlan, promiscuous port	-

Command Mode

Interface Configuration

Default

By default the switch port's mode is access vlan.

Usage

To configure the switch port's mode as private vlan, use the "switchport mode private-vlan" command in interface mode.

This can only be configured on a switchport.

Examples

The following example shows how to configure the switch port mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport mode private-vlan promiscuous
```

Related Commands

switchport private-vlan

11.18.2 switchport private-vlan

Command Purpose

To configure the primary and secondary vlan of a private vlan, use the "switchport private-vlan" command in interface mode.

Use the "no" form of this command to restore the default value.

Command Syntax

switchport private-vlan *VLAN_ID* (isolate | community-vlan *VLAN_ID* |)

Parameter	Parameter Description	Parameter Value
private-vlan VLAN_ID	Set private primary vlan	1-4094
isolate	Set as isolate mode	-
community-vlan VLAN_ID	Set communtiy vlan	1-4094

Command Mode

Interface Configuration

Default

By default, the primary vlan is 1.

If the switchport mode is private-vlan host, the default mode is isolate; Or else the switchport mode is promiscuous

Usage

To configure the primary and secondary vlan of a private vlan, use the "switchport private-vlan" command in interface mode.

This can only be configured on a switchport.

Examples

The following example shows how to configure the private vlan:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan 1 isolate
Switch(config-if)# quit
Switch(config)# interface eth-0-2
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan 1 community-vlan 2
Switch(config-if)# quit
Switch(config)# interface eth-0-3
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan 1
```

Related Commands

switchport mode private-vlan

11.18.3 show private-vlan**Command Purpose**

To display the private-vlan configure, use the show private-vlan command in privileged Privileged EXEC.

Command Syntaxshow private-vlan (vlan *VLAN_ID* | interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
VLAN_ID	Show by primary vlan	1-4094
IFNAME	Show by interface	Support physical/ aggregation ports

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

The following example shows the result of this command:

```
Switch# show private-vlan
```

Primary	Secondary	Type	Ports
1	N/A	promiscuous	eth-0-3
1	N/A	isolate	eth-0-1
1	2	community	eth-0-2

```
DUT1# show private-vlan vlan 1
```

Primary	Secondary	Type	Ports
1	N/A	promiscuous	eth-0-3
1	N/A	isolate	eth-0-1
1	2	community	eth-0-2

```
DUT1# show private-vlan interface eth-0-1
```

```
Private vlan mode: isolate
```

```
Primary vlan id : 1
```

Related Commands

```
switchport mode private-vlan
```

```
switchport private-vlan
```

11.19 DDOS Commands

11.19.1 ip icmp intercept

Command Purpose

To configure the system to resist ICMP flood attack, use the ip icmp intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip icmp intercept ( maxcount NUMBER | )
```

```
no ip icmp intercept
```

Parameter	Parameter Description	Parameter Value
NUMBER	Specify max counter of received packets per second	0-1000

Command Mode

Global Configuration

Default

By default, ip icmp intercept is unset.

If the maxcount is not specified , the default count is 500.

Usage

Use this command if you want to set the system to limit the ICMP packet rate.

Examples

The following example shows how to configure the ip icmp intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip icmp intercept maxcount 100
```

The following example unset the ip icmp intercept:

```
Switch# configure terminal
```

```
Switch(config)# no ip icmp intercept
```

Related Commands

```
show ip-intercept config
```

11.19.2 ip smurf intercept**Command Purpose**

To configure the system to resist smurf attack, use the ip smurf intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip smurf intercept
```

```
no ip smurf intercept
```

Command Mode

Global Configuration

Default

By default, ip smurf intercept is unset.

Usage

Use this command if you want to set the system to resist smurf attack.

Examples

The following example shows how to configure the ip smurf intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip smurf intercept
```

The following example unset the ip smurf intercept::

```
Switch# configure terminal
```

```
Switch(config)# no ip smurf intercept
```

Related Commands

```
show ip-intercept config
```

11.19.3 ip fraggle intercept**Command Purpose**

To configure the system to resist fraggle attack, use the ip fraggle intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip fraggle intercept
```

```
no ip fraggle intercept
```


Command Mode

Global Configuration

Default

By default, ip fraggle intercept is unset.

Usage

Use this command if you want to set the system to resist fraggle attack.

Examples

The following example shows how to configure the ip fraggle intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip fraggle intercept
```

The following example unset the ip fraggle intercept:

```
Switch# configure terminal
```

```
Switch(config)# no ip fraggle intercept
```

Related Commands

show ip-intercept config

11.19.4 ip udp intercept**Command Purpose**

To configure the system to resist UDP flood attack, use the ip udp intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip udp intercept (maxcount *NUMBER* |)

no ip udp intercept

Parameter	Parameter Description	Parameter Value
NUMBER	Specify max counter of received packets per second	0-1000

Command Mode

Global Configuration

Default

By default, ip udp intercept is unset.

If the maxcount is not specified , the default count is 500.

Usage

Use this command if you want to set the system to limit the UDP packet rate.

Examples

The following example shows how to configure the ip udp intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip udp intercept maxcount 100
```

The following example unset the ip udp intercept:

```
Switch# configure terminal
```

```
Switch(config)# no ip udp intercept
```

Related Commands

show ip-intercept config

11.19.5 ip tcp intercept

Command Purpose

To configure the system to resist SYN flood attack, use the ip tcp intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip tcp intercept (maxcount number |)

no ip tcp intercept

Parameter	Parameter Description	Parameter Value
NUMBER	Specify max counter of received packets per second	0-1000

Command Mode

Global Configuration

Default

By default, ip tcp intercept is unset.

If the maxcount is not specified , the default count is 500.

Usage

Use this command if you want to set the system to limit the TCP packet rate with only SYN bit set.

Examples

The following example shows how to configure the ip tcp intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip tcp intercept maxcount 100
```

The following example unset the ip tcp intercept:

```
Switch# configure terminal
```

```
Switch(config)# no ip tcp intercept
```

Related Commands

```
show ip-intercept config
```

11.19.6 ip small-packet intercept

Command Purpose

To configure the system to filter the small packet, use the ip small-packet command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip small-packet intercept (length number |)

no ip small-packet intercept

Parameter	Parameter Description	Parameter Value
NUMBER	Specify length of small packet	28-65535

Command Mode

Global Configuration

Default

By default, ip small-packet intercept is unset.

If the length is not specified , the default value is 28 bytes.

Usage

Use this command if you want to set the system to drop the packet which length is less than the configured value.

Examples

The following example configures the ip small-packet intercept:

```
Switch# configure terminal
```

```
Switch(config)# ip small-packet intercept length 32
```

The following example unset the ip small-packet intercept:

```
Switch# configure terminal
```

```
Switch(config)# no small-packet intercept
```

Related Commands

```
show ip-intercept config
```

11.19.7 ip maceq intercept**Command Purpose**

To configure the system to intercept the packet whose source MAC equals to destination MAC, use the ip maceq intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip maceq intercept
```

```
no ip maceq intercept
```

Command Mode

Global Configuration

Default

By default, ip mac equal intercept is unset.

Usage

Use this command if you want to set the system to drop the packet whose source MAC equals to destination MAC.

Examples

The following example configures the ip intercept mac equals:

```
Switch# configure terminal
```

```
Switch(config)# ip maceq intercept
```

The following example unset the ip intercept mac equals:

```
Switch# configure terminal
```

```
Switch(config)# no ip maceq intercept
```

Related Commands

```
show ip-intercept config
```

11.19.8 ip ipeq intercept**Command Purpose**

To configure the system to intercept the packet whose source IP address equals to destination IP address, use the ip ipeq intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ip ipeq intercept
```

```
no ip ipeq intercept
```

Command Mode

Global Configuration

Default

By default, ip ip equal intercept is unset.

Usage

Use this command if you want to set the system to drop the packet whose source IP address equals to destination IP address.

Examples

The following example configures the ip intercept ip equal:

```
Switch# configure terminal
Switch(config)# ip ipeq intercept
```

The following example unset the ip intercept ip equal:

```
Switch# configure terminal
Switch(config)# no ip ipeq intercept
```

Related Commands

show ip-intercept config

11.19.9 show ip-intercept config**Command Purpose**

To display the ip intercept configurations, use the show ip-intercept config command in privileged Privileged EXEC.

Command Syntax

show ip-intercept config

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display ip intercept configurations.

Examples

The following example shows the configuration of ip intercept:

```
Switch# show ip-intercept config
```

Current DDoS Prevent configuration:

```
=====
ICMP Flood Intercept      :Enable  Maxconut:100
UDP Flood Intercept      :Enable  Maxconut:100
SYN Flood Intercept      :Enable  Maxconut:100
Small-packet Attack Intercept :Enable  Packet Length:32
Sumrf Attack Intercept   :Enable
Fraggle Attack Intercept :Enable
MAC Equal Intercept      :Disable
IP Equal Intercept       :Disable
```

Related Commands

show ip-intercept config

11.19.10 show ip-intercept statistics

Command Purpose

To display the statistics of the intercept packets, use the show ip-intercept statistics command in privileged Privileged EXEC.

Command Syntax

```
show ip-intercept statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display ip intercept statistics.

Examples

The following is sample output from the show ip-intercept statistics command::

```
Switch# show ip-intercept statistics
```

```
Current DDoS Prevent statistics:
```

```
=====
Resist Small-packet Attack packets number    : 108
Resist ICMP Flood packets number             : 0
Resist Smurf Attack packets number           : 0
Resist SYN Flood packets number              : 0
Resist Fraggle Attack packets number         : 0
Resist UDP Flood packets number              : 0
```

Related Commands

```
clear ip-intercept statistics
```

11.19.11 clear ip-intercept statistics

Command Purpose

To clear the statistics of the intercept packets, use the clear ip-intercept statistics command in privileged Privileged EXEC.

Command Syntax

```
clear ip-intercept statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to clear ip intercept statistics.

Examples

The following example displays how to use clear ip-intercept statistics command::

```
Switch# clear ip-intercept statistics
```

```
Switch# show ip-intercept statistics
```

Current DDoS Prevent statistics:

```
=====
Resist Small-packet Attack packets number    : 0
Resist ICMP Flood packets number             : 0
Resist Smurf Attack packets number           : 0
Resist SYN Flood packets number              : 0
Resist Fraggle Attack packets number         : 0
Resist UDP Flood packets number              : 0
```

Related Commands

show ip-intercept statistics

11. 20 Key Chain Commands

11.20.1 key chain

Command Purpose

To create a keychain, use the key chain command in global configuration mode. To delete a keychain, use the no form of this command.

Command Syntax

key chain *WORD*

no key chain *WORD*

Parameter	Parameter Description	Parameter Value
WORD	The name of keychain	String with up to 20 characters

Command Mode

Global Configuration

Default

No keychain is created.

Usage

Routing protocols and network management applications often use keychain to enhance security while communicating with peers. For the detail of these configurations, see relevant chapters of user guide.

Examples

The following example shows how to create a keychain:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)#
```

Related Commands

key

key-string

show key chain

11.20.2 Key

Command Purpose

To create a key in a keychain, use the key command in keychain configuration mode. To delete a key from a keychain, use the no form of this command.

Command Syntax

key *KEY_ID*

no key *KEY_ID*

Parameter	Parameter Description	Parameter Value
KEY_ID	key id	0-31

Command Mode

Key Chain Configuration

Default

There is no key in a keychain.

Usage

The key will not be used unless key string was configured.

Examples

The following example shows how to create a key:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 1
```

Related Commands

key chain

key-string

accept-lifetime

send-lifetime

11.20.3 key-string

Command Purpose

To configure key string for a key, use key-string command in key configuration mode. To delete configuration, use the no form of this command.

Command Syntax

key-string *LINE*

no key-string *LINE*

Parameter	Parameter Description	Parameter Value
LINE	Key string	String with up to 255 characters

Command Mode

Key Configuration

Default

The key string is not be configured.

Usage

This command is used to configure key string for a key and then this key will be valid for ever if there is no lifetime set.

Examples

The following example shows how to configure key-string:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# key-string ##test_keywords##
```

Related Commands

key
accept-lifetime
send-lifetime

11.20.4 accept-lifetime

Command Purpose

To configure the accept lifetime for a key, use accept-lifetime command in key configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

```
accept-lifetime START-TIME EXPIRE-TIME
no accept-lifetime
```

Parameter	Parameter Description	Parameter Value
START-TIME	The start of accept lifetime	The start of accept lifetime its format should like "HH:MM:SS <1-31> MONTH <1993-2035>" or "HH:MM:SS MONTH <1-31> <1993-2035>" and MONTH should be First three letters of the month
EXPIRE-TIME	The end of accept lifetime	The end of accept lifetime, its format should like "HH:MM:SS <1-31> MONTH <1993-2035>"; "HH:MM:SS MONTH <1-31> <1993-2035> "; "Infinite" or "duration <1-2147483646>" and MONTH should be First three letters of the month

Command Mode

Key Configuration

Default

No accept lifetime is configured

Usage

This command is used to configure accept lifetime for a key which will be invalid after lifetime expired.

Examples

The following example shows how to configure accept-lifetime:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# accept-lifetime 0:0:1 2 jan 2012 infinite
```

Related Commands

key
key-string

11.20.5 send-lifetime

Command Purpose

To configure the send lifetime for a key, use send-lifetime command in key configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

send-lifetime *START-TIME EXPIRE-TIME*

no send-lifetime

Parameter	Parameter Description	Parameter Value
START-TIME	The start of send lifetime	The start of send lifetime, its format should like "HH:MM:SS <1-31> MONTH <1993-2035>" or "HH:MM:SS MONTH <1-31> <1993-2035>" and MONTH should be First three letters of the month
EXPIRE-TIME	The end of send lifetime	The end of send lifetime,its format should like "HH:MM:SS <1-31> MONTH <1993-2035>", "HH:MM:SS MONTH <1-31> <1993-2035>", "Infinite" or "duration <1-2147483646>" and MONTH should be First three letters of the month

Command Mode

Key Configuration

Default

No send lifetime is configured

Usage

This command is used to configure send lifetime for a key which will be invalid after lifetime expired.

Examples

The following example shows how to configure send-lifetime:

```
Switch# configure terminal
Switch(config)# key chain test
Switch(config-keychain)# key 2
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite
```

Related Commands

key
key-string

11.20.6 show key chain

Command Purpose

To show information of keychain, use show key chain command.

Command Syntax

show key chain (*WORD* |)

Parameter	Parameter Description	Parameter Value
<i>WORD</i>	The name of keychain	String with up to 20 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display keychain:

```
Switch# show key chain test

key chain test:
  key 1 -- text "key-string ##test_keywords_1##"
    accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
    send-lifetime <always valid> - <always valid> [valid now]
  key 2 -- text "key-string ##test_keywords_2##"
    accept-lifetime <always valid> - <always valid> [valid now]
    send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

Related Commands

key chain

11.21 Port-block Commands

11.21.1 port-block

Command Purpose

To configure port block, use the port-block command in interface configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

no port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

Parameter	Parameter Description	Parameter Value
known-unicast	Specify that known unicast traffic should be blocked	-
known-multicast	Specify that known multicast traffic should be blocked	-
unknown-unicast	Specify that unknown unicast traffic should be blocked	-
unknown-multicast	Specify that unknown multicast traffic should be blocked	-
broadcast	Specify that broadcast traffic should be blocked	-

Command Mode

Interface Configuration

Default

Unknown or known multicast and unicast traffic is not blocked.

Broadcast traffic is not blocked.

Usage

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or non protected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# port-block known-unicast
```

Related Commands

show port-block (interface IFPHYSICAL | interface IFAGG |)

11.21.2 show port-block

Command Purpose

Use this command to display the port-block configuration.

Command Syntax

show port-block (interface IFNAME |)

Parameter	Parameter Description	Parameter Value
IFNAME	Specify the interface	Support physical/ aggregation ports

Command Mode

Privileged EXEC

Default

N/A

Usage

If the interface is not specified, all interfaces should be displayed.

Examples

This example shows how to show port-block configuration in Privileged Privileged EXEC:

```
Switch# show port-block interface eth-0-1
```

Related Commands

port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

11.22 Device Management Security Commands

11.22.1 ip telnet server acl

Command Purpose

To deny specified telnet client IP, use this command in configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

```
ip telnet server acl NAME
```

```
no ip telnet server acl
```

Parameter	Parameter Description	Parameter Value
NAME	access-list name	String with up to 40 characters

Command Mode

Global Configuration

Default

No acl is specified

Usage

Use this command to deny specified telnet client IP.

The access-list should be created before using this command.

Examples

This example shows how to enable telnet acl, which deny telnet client with source IP 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list telnetACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# exit
Switch(config)# ip telnet server acl telnetACL
```

Related Commands

None

11.22.2 ip ssh server acl

Command Purpose

To deny specified SSH client IP, use this command in configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

ip ssh server acl *NAME*

ip no ssh server acl

Parameter	Parameter Description	Parameter Value
NAME	access-list name	String with up to 40 characters

Command Mode

Global Configuration

Default

No acl is specified

Usage

Use this command to deny specified SSH client IP.

The access-list should be created before using this command.

Examples

This example shows how to enable SSH acl, which deny SSH client with source IP 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ip access-list telnetACL
Switch(config-ip-acl)# 10 deny tcp host 1.1.1.1 any
Switch(config-ip-acl)# exit
Switch(config)# ip ssh server acl telnetACL
```

Related Commands

None

11.22.3 service password-encryption**Command Purpose**

To encrypt password of users and line vty, use this command in configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

service password-encryption

no service password-encryption

Command Mode

Global Configuration

Default

None

Usage

Use this command to encrypt password of users and line vty, after this command is configured, existed password or new configured password will be encrypted.

Examples

The following example shows how to encrypt user password:

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch# show running-config
username admin privilege 4 password 8 56ab359baafb02a3
```

Related Commands

None

Chapter 12 IPv6 Security Commands

12.1 DHCPv6 Snooping Commands

12.1.1 clear dhcpv6 snooping bindings learning

Command Purpose

Use the clear dhcpv6 snooping bindings learning privileged EXEC command on the switch to clear the dynamic DHCPv6 binding items.

Command Syntax

clear dhcpv6 snooping bindings (learning | manual) (ipv6 *IP-ADDRESS* | mac *MAC-ADDRESS* | vlan *VLAN-ID* | interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
ipv6 <i>IP-ADDRESS</i>	Clear the binding entry with the IPv6 address	IPv6 Address
mac <i>MAC-ADDRESS</i>	Clear the binding entry with the MAC address	MAC address
vlan <i>VLAN-ID</i>	Clear the binding entry with the VLAN	1-4094
interface <i>IFNAME</i>	Clear the binding entry with the Interface	Support physical/aggregation ports

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to clear DHCPv6 snooping binding.

Examples

This example shows how to clear all DHCPv6 snooping binding learning items:

```
Switch# clear dhcpv6 snooping bindings learning
```

Related Commands

show dhcpv6 snooping binding

12.1.2 clear dhcpv6 snooping statistics

Command Purpose

Use the clear dhcpv6 snooping statistics privileged EXEC command on the switch to clear the DHCPv6 snooping statistics counters.

Command Syntax

```
clear dhcpv6 snooping statistics
```

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to clear DHCPv6 snooping statistics.

Examples

This example shows how to clear the DHCPv6 snooping statistics counters:

```
Switch# clear dhcpv6 snooping statistics
```

Related Commands

```
show dhcpv6 snooping statistics
```

12.1.3 dhcpv6 snooping

Command Purpose

Use the dhcpv6 snooping global configuration command on the switch to globally enable DHCPv6 snooping.
Use the no form of this command to return to the default setting.

Command Syntax

```
dhcpv6 snooping  
no dhcpv6 snooping
```


Command Mode

Global Configuration

Default

DHCPv6 snooping is disabled.

Usage

For any DHCPv6 snooping configuration to take effect, you must globally enable DHCPv6 snooping. DHCPv6 snooping is not active until you enable snooping on a VLAN by using the `dhcpv6 snooping vlan` global configuration command.

Examples

This example shows how to enable DHCPv6 snooping:

```
Switch# configure terminal
Switch(config)# dhcpv6 snooping
```

You can verify your settings by entering the `show dhcpv6 snooping config` privileged EXEC command:

Related Commands

`dhcpv6 snooping vlan`
`show dhcpv6 snooping config`

12.1.4 dhcpv6 snooping binding

Command Purpose

Use the `dhcpv6 snooping binding` global configuration command on the switch to configure the DHCPv6 snooping binding database and to add binding entries to the database.

Command Syntax

`dhcpv6 snooping binding mac MAC-ADDRESS vlan VLAN-ID ipv6 IP-ADDRESS interface IFNAME expiry SECONDS`
`no dhcpv6 snooping bindings ( ipv6 IP-ADDRESS | mac MAC-ADDRESS | vlan VLAN-ID | interface IFNAME | )`

Parameter	Parameter Description	Parameter Value
mac MAC-ADDRESS	Specify a MAC address	MAC address
vlan VLAN-ID	Specify a VLAN number.	1-4094
ipv6 IP-ADDRESS	Specify an IPv6 address	IPv6 Address
interface IFNAME	Specify an interface on which to add or delete a binding entry	Support physical/aggregation ports

Parameter	Parameter Description	Parameter Value
expiry SECONDS	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is 0 to 86400	0-86400 seconds

Command Mode

Global Configuration

Default

No default database is defined.

Usage

Use this command when you are testing or debugging the switch.

In the DHCPv6 snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the show dhcpv6 snooping binding privileged EXEC command to display the configured bindings.

Examples

This example shows how to generate a DHCPv6 binding with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# configure terminal
```

```
Switch(config)# dhcpv6 snooping binding mac 0001.000c.01ef vlan 1 ipv6 2001:1::1 interface eth-0-1 expiry 1000
```

Related Commands

show dhcpv6 snooping binding

12.1.5 dhcpv6 snooping database

Command Purpose

Use the dhcpv6 snooping database global configuration command on the switch to configure the DHCPv6 snooping binding database agent. Use the no form of this command to reset the write-delay value.

Command Syntax

dhcpv6 snooping database auto-save interval *SECONDS*

Parameter	Parameter Description	Parameter Value
interval SECONDS	Specify the interval (in seconds) that how long to save the binding database.	15-2000 seconds

Command Mode

Global Configuration

Default

Default interval is 600 seconds.

Usage

The DHCPv6 snooping database is save as flash:/dhcpv6snooping.

Examples

The following is sample output from the dhcpv6 snooping database command:

```
Switch# configure terminal
Switch(config)# dhcpv6 snooping database auto-save interval 120
```

Related Commands

dhcpv6 snooping

dhcpv6 snooping binding

12.1.6 dhcpv6 snooping trust

Command Purpose

Use the dhcpv6 snooping trust interface configuration command on the switch to configure a port as trusted for DHCPv6 snooping purposes.

Use the no form of this command to return to the default setting.

Command Syntax

dhcpv6 snooping trust

no dhcpv6 snooping trust

Command Mode

Interface Configuration

Default

DHCPv6 snooping trust is disabled.

Usage

Configure as trusted ports those that are connected to a DHCPv6 server or to other switches or routers. Configure as entrusted ports those that are connected to DHCPv6 clients.

Examples

This example shows how to enable DHCPv6 snooping trust on a port:

```
Switch# configure terminal
Switch(config)# interface eth-0/1
Switch(config-if)# dhcpv6 snooping trust
```

Related Commands

show dhcpv6 snooping trusted-sources

12.1.7 dhcpv6 snooping vlan

Command Purpose

Use the dhcpv6 snooping vlan global configuration command on the switch to enable DHCPv6 snooping on a VLAN. Use the no form of this command to return to the default setting.

Command Syntax

dhcpv6 snooping vlan *VLAN-RANGE*

no dhcpv6 snooping vlan *VLAN-RANGE*

Parameter	Parameter Description	Parameter Value
VLAN-RANGE	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping.	1-4094

Command Mode

Global Configuration

Default

DHCPv6 snooping is disabled on all VLANs.

Usage

You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.

You must first globally enable DHCPv6 snooping before enabling DHCPv6 snooping on a VLAN.

Examples

This example shows how to enable DHCPv6 snooping on VLAN 10:

```
Switch# configure terminal
Switch(config)# dhcpv6 snooping vlan 10
```

Related Commands

show dhcpv6 snooping config

12.1.8 debug dhcpv6 snooping

Command Purpose

Use this command to turn on the debug switches of dhcpv6 snooping module.

To restore the default, use the no form of this command

Command Syntax

debug dhcpv6 snooping (events | error | dump | packet | all)

no debug dhcpv6 snooping (events | error | dump | packet | all)

Parameter	Parameter Description	Parameter Value
events	Snooping events	-
error	Error DHCPv6 message	-
packet	DHCPv6 message fields	-
dump	Dump message in hex format	-
all	Turn all debugging on	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.

Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcpv6 snooping debug switches:

```
Switch# debug dhcpv6 snooping all
```

Related Commands

terminal monitor

show logging buffer

12.1.9 show dhcpv6 snooping binding

Command Purpose

Use the show dhcpv6 snooping binding privileged EXEC command to display the DHCPv6 snooping binding database and configuration information for all interfaces on a switch.

Command Syntax

show dhcpv6 snooping binding ((all | manual | learning) (ipv4 *IP-ADDRESS* | mac *MAC-ADDRESS* | vlan *VLAN-ID* | interface *IFNAME* |) summary |)

Parameter	Parameter Description	Parameter Value
all	Display all entries	-
manual	Display static entries	-
learning	Display dynamic entries	-
mac <i>MAC-ADDRESS</i>	Specify MAC address	MAC address
vlan <i>VLAN-ID</i>	Specify a VLAN number.	1-4094
ipv4 <i>IP-ADDRESS</i>	Specify an IP address	IPv4 Address
interface <i>IFNAME</i>	Specify an interface on which to add or delete a binding entry	Support physical/aggregation ports
summary	Display summary information of DHCPv6 snooping bindings	-

Command Mode

Privileged EXEC

Default

None

Usage

If DHCPv6 snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Examples

The following is sample output from the show dhcpv6 snooping binding command:

```
Switch# show dhcpv6 snooping binding all
```

DHCPv6 snooping binding table:

VLAN	MAC Address	Interface	Lease(s)	IPv6 Address

1	0001.0001.0001	eth-0-2	static	1:1::1:1

```
Switch# show dhcpv6 snooping binding summary
```

Total 1 DHCPv6 snooping binding entries

0 learning entry, 1 configured entry

Related Commands

dhcpv6 snooping binding

12.1.10 show dhcpv6 snooping config

Command Purpose

Use the show dhcpv6 snooping privileged EXEC command to display the DHCPv6 snooping configuration.

Command Syntax

```
show dhcpv6 snooping config
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping config command:

```
Switch# show dhcpv6 snooping config
```

```
dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 3
```

Related Commands

```
dhcpv6 snooping
dhcpv6 snooping vlan
```

12.1.11 show dhcpv6 snooping trusted-sources

Command Purpose

Use the show dhcpv6 snooping trusted-sources privileged EXEC command to display the DHCPv6 snooping trusted interface.

Command Syntax

```
show dhcpv6 snooping trusted-sources
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the trusted interface of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping trusted-sources command:

```
Switch# show dhcpv6 snooping trusted-source
```

```
List of DHCPv6 snooping trusted interface(s):
```

```
=====
eth-0-20
```

Related Commands

```
dhcpv6 snooping trust
```


12.1.12 show dhcpv6 snooping statistics

Command Purpose

Use the show dhcpv6 snooping statistics privileged EXEC command to display DHCPv6 snooping statistics.

Command Syntax

```
show dhcpv6 snooping statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the statistics of DHCPv6 snooping.

Examples

The following is sample output from the show dhcpv6 snooping statistics command:

```
Switch# show dhcpv6 snooping statistics
```

```
DHCPv6 snooping statistics:
```

```
=====
DHCPv6 packets                137
Packets forwarded             137
Packets invalid                0
Packets dropped                0
```

Related Commands

```
clear dhcpv6 snooping statistics
```

Chapter 13 Reliability Commands

13.1 BHM Commands

13.1.1 sysmon enable

Command Purpose

Use this command to enable system monitor. Use the no command to disable system monitor.

Command Syntax

```
sysmon enable  
no sysmon enable
```

Command Mode

Global Configuration

Default

Sysmon is enabled by default.

Usage

None

Examples

The following example shows how to enable system monitor:

```
Switch# configure terminal  
Switch(config)# sysmon enable
```

Related Commands

```
show sysmon
```

13.1.2 show sysmon

Command Purpose

Use this command to show system monitor information.

Command Syntax

```
show sysmon
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display system monitor status:

```
Switch# show sysmon
```

```
System monitor enable.
```

Related Commands

sysmon enable

13.1.3 heart-beat-monitor enable**Command Purpose**

Use this command to enable heart beat monitor. Use the no command to disable heart beat monitor.

Command Syntax

heart-beat-monitor enable

no heart-beat-monitor enable

Command Mode

Global Configuration

Default

The default of heart beat monitor is enabled.

Usage

None

Examples

The following example shows how to enable heart beat monitor:

```
Switch# configure terminal
Switch(config)# heart-beat-monitor enable
```

Related Commands

show heart-beat-monitor

13.1.4 heart-beat-monitor reactivate

Command Purpose

Use this command to specify a reactivation after process crash.

Command Syntax

heart-beat-monitor reactivate (reload system | shutdown port | warning)

Parameter	Parameter Description	Parameter Value
reload system	reload system	-
shutdown port	shutdown all port when system crash	-
warning	print warning on screen	-

Command Mode

Global Configuration

Default

The default reactivation is to reload system.

Usage

None

Examples

The following example shows how to set heart-beat-monitor the reactivation:

```
Switch# configure terminal
Switch(config)# heart-beat-monitor reactivate reload system
```

Related Commands

show heart-beat-monitor

13.1.5 show heart-beat-monitor

Command Purpose

Use this command to show heart beat monitor status.

Command Syntax

show heart-beat-monitor

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to show system monitor information:

```
Switch# show heart-beat-monitor
heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.
```

Related Commands

heart-beat-monitor enable

heart-beat-monitor reactivate

13.2 CPU Traffic Limit Commands

13.2.1 cpu-traffic-limit total rate

Command Purpose

Use this command to set the total rate of all streams destined to CPU. Use the no form of this command to set the total rate to the default value.

Command Syntax

cpu-traffic-limit total rate *RATE_RANGE*

no cpu-traffic-limit total rate

Parameter	Parameter Description	Parameter Value
RATE_RANGE	Rate of all streams destined to cpu in pps	0-1000000

Command Mode

Global Configuration

Default

2048 pps

Usage

N/A

Examples

This example shows how to configure cpu-traffic-limit total rate:

```
Switch# configure terminal
```

```
Switch(config)# cpu-traffic-limit total rate 3000
```

This example shows how to reset cpu-traffic-limit total rate:

```
Switch# configure terminal
```

```
Switch(config)# no cpu-traffic-limit total rate
```

Related Commands

show cpu traffic-limit

13.2.2 cpu-traffic-limit reason rate

Command Purpose

Use this command to set the individual limit rate for the stream carried with this reason. Use the no form of this command to set the individual limit rate of the reason to its default value.

Command Syntax

```
cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ssh | telnet | mlag | tcp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | fwd-to-cpu | uddl | bfd-learning } rate RATE_RANGE
no cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress | fwd-to-cpu | uddl | bfd-learning } rate
```

Parameter	Parameter Description	Parameter Value
bpdu	Reason for BPDU protocols packets(including STP, RSTP, MSTP)	-
slow-protocol	Reason for slow protocol packets.(including EFM, LACP)	-
eapol	Reason for Dot1x protocol packets	-
erps	Reason for ERPS protocol packets Reason for ERPS protocol packets	-
arp	Reason for ARP protocol packets	-
dhcp	Reason for DHCP protocol packets	-
rip	Reason for RIP protocol packets	-
bgp	Reason for BGP protocol packets	-
ldp	Reason for LDP protocol packets	-
ospf	Reason for OSPF protocol packets	-
pim	Reason for PIM protocol packets	-
vrrp	Reason for VRRP protocol packets	-
ssh	Reason for SSH protocol packets	-
telnet	Reason for Telnet protocol packets	-
mlag	Reason for MLAG protocol packets	-
tcp	Reason for TCP protocol packets	-
ipda	Reason for packets with IPDA destination to router itself	-
icmp-redirect	Reason for redirecting ICMP	-
learning-full	Reason for learning cache is full	-
mcast_rpf_fail	Reason for multi-cast packets with rpf fail	-
macsa-mismatch	Reason for packets that are discarded for source mac is learned from another security port	-

Parameter	Parameter Description	Parameter Value
port-security-discard	Reason for packets that are discarded for fdb number equals to allowed maximum number of security port	-
vlan-security-discard	Reason for packets that are discarded for fdb number equals to allowed maximum number on the specified vlan	-
ip-mtu-fail	Ip mtu fail	-
ip-option	Reason for IP packets with optional fields	-
ucast-ttl-fail	Reason for ucast ip packets with fail TTL	-
mpls-ttl-fail	Reason for mpls packets with fail TTL	-
igmp	Reason for IGMP or igmp snooping packets	-
sflow-ingress	Reason for sflow sampled packets at ingress direction	-
sflow-egress	Reason for sflow sampled packets at egress direction	-
fwd-to-cpu	Reason for packets forwarding to cpu	-
bfd-learning	Reason for bfd learning packets	-
RATE_RANGE	Individual rate of streams destined to cpu carried with the reason in kbps	0-1000000
mld	mld packets or mld snooping packets	-
dot1x-mac-bypass	mac auth bypass packets	-

Command Mode

Global Configuration

Default

Reason	Rate(pps)	Reason	Rate(pps)
bpdu	64	icmp-redirect	128
slow-protocol	128	mcast-rpf-fail	128
eapol	128	macsa-mismatch	128
erps	128	port-security-discard	128
smart-link	128	vlan-security-discard	128

Reason	Rate(pps)	Reason	Rate(pps)
arp	640	udld	128
dhcp	128	ip-mtu-fail	64
rip	64	fwd-to-cpu	64
ldp	512	ip-option	512
ospf	256	ucast-ttl-fail	64
pim	128	mpls-ttl-fail	64
vrrp	512	igmp	128
ssh	64	telnet	64
mlag	1024	tcp	64
ipda	1024	sflow-ingress	128
sflow-egress	128	bfd-learning	128
sflow-egress	128	bfd-learning	128

Usage

ssh/telnet/mlag is useful when enable cpu-traffic-optimize.

Examples

This example shows how to configure individual rate for BPDU PDU:

```
Switch# configure terminal
```

```
Switch(config)# cpu-traffic-limit reason bpdu rate 300
```

This example shows how to reset individual rate for BPDU PDU:

```
Switch# configure terminal
```

```
Switch(config)# no cpu-traffic-limit reason bpdu rate
```

Related Commands

```
show cpu traffic-limit
```

13.2.3 cpu-traffic-limit reason class

Command Purpose

Use this command to set the priority class for the stream carried with the reason. Use the no form of this command to set the priority class of the reason to its default value.

Command Syntax

```
cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ssh | telnet | mlag | tcp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | udld | bfd-learning } class CLASS_RANGE
```

no cpu-traffic-limit reason { bpdu | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | vrrp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | mtu-dontfrag | mtu-frag | ip-option | ucast-ip-ttl-fail | mpls-ttl-fail | igmp | sflow-ingress | sflow-egress | udld | bfd-learning } class

Parameter	Parameter Description	Parameter Value
CLASS_RANGE	Priority of the stream carried with this reason. Reason with class 3 has the highest priority.	0-3

Command Mode

Global Configuration

Default

Reason	class	Reason	class
bpdu	3	icmp-redirect	0
slow-protocol	1	mcast-rpf-fail	1
eapol	0	macsa-mismatch	0
erps	2	port-security-discard	0
smart-link	2	vlan-security-discard	0
arp	1	udld	3
dhcp	0	mtu-dontfrag	0
rip	1	mtu-frag	0
ldp	1	sflow-ingress	0
ospf	1	ip-option	0
pim	1	ucast-ttl-fail	0
vrrp	1	mpls-ttl-fail	0
igmp	2	ssh	3
telnet	3	mlag	1
tcp	2	ipda	0
igmp	2	mld	2
sflow-egress	0	dot1x-mac-bypass	2
fwd-to-cpu	0	bfd-learning	1
fwd-to-cpu	0	bfd-learning	1

Usage

The reason with the highest priority class will get preference treatment when dealing with scheduling. ssh/telnet/mlag is useful when enable cpu-traffic-optimize.

Examples

This example shows how to configure priority class for BPDU:

```
Switch# configure terminal
```

```
Switch(config)# cpu-traffic-limit reason bpdu class 3
```

Related Commands

show cpu traffic-limit

13.2.4 show cpu traffic-limit

Command Purpose

Use this command to show the CPU traffic-limit configurations.

Command Syntax

show cpu traffic-limit

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows cpu traffic-limit configurations:

```
DUT2# show cpu traffic-limit
```

reason	rate (pps)	class
dot1x-mac-bypass	64	2
bpdu	64	3
slow-protocol	128	1
eapol	128	0
erps	128	2
smart-link	128	2
udld	128	3
loopback-detection	64	3
arp	256	1
dhcp	128	0
rip	64	1
ldp	512	1

ospf	256	1
pim	128	1
bgp	256	1
vrrp	512	1
rsvp	512	1
ssh	64	3
telnet	64	3
mlag	1024	0
tcp	64	2
ipda	1024	0
icmp-redirect	128	0
mcast-rpf-fail	128	1
macsa-mismatch	128	0
port-security-discard	128	0
vlan-security-discard	128	0
ip-mtu-fail	64	0
bfd-learning	128	1
ptp	512	2
ip-option	512	0
tunnel-gre-keepalive	64	0
ucast-ttl-fail	64	0
mpls-ttl-fail	64	0
igmp	128	2
sflow-ingress	128	0
sflow-egress	128	0
fwd-to-cpu	64	0
l2protocol-tunnel	1024	0
mirror-to-cpu	256	0
mpls-tp-pwoam	128	2
Total rate:	2048 (pps)	

Related Commands

cpu-traffic-limit total rate

cpu-traffic-limit reason rate

13.3 CPU Traffic Statistics Commands

13.3.1 cpu-traffic-statistics time

Command Purpose

Use this command to set the CPU receive packets or CPU transmit packets statistics time.

Command Syntax

cpu-traffic-statistics time *RATE-TIME*

Parameter	Parameter Description	Parameter Value
RATE-TIME	Rate of statistics time	1-10 seconds

Command Mode

Global Configuration

Default

5 s

Usage

N/A

Examples

This example shows how to configure cpu-traffic-statistics time:

```
Switch# configure terminal
Switch(config)# cpu-traffic-statistics time 2
```

Related Commands

N/A

13.3.2 no cpu-traffic-statistics time

Command Purpose

Use this command to reset the CPU receive packets or CPU transmit packets statistics time.

Command Syntax

no cpu-traffic-statistics time

Command Mode

Global Configuration

Default

N/A

Usage

N/A

Examples

This example shows how to reset cpu-traffic-statistics time:

```
Switch# configure terminal
Switch(config)# no cpu-traffic-statistics time
```

Related Commands

N/A

13.3.3 show cpu traffic- statistics receive

Command Purpose

Use this command to show CPU receive packets by reason.

Command Syntax

show cpu traffic-statistics receive (bpdud | slow-protocol | eapol | erps | smart-link | arp | dhcp | rip | ldp | ospf | pim | bgp | vrrp | ssh | telnet | mlag | tcp | ipda | icmp-redirect | mcast-rpf-fail | macsa-mismatch | port-security-discard | vlan-security-discard | ip-mtu-fail | ip-option | ucast-ttl-fail | sflow-ingress | sflow-egress | igmp | udld | dot1x-mac-bypass | l2protocol-tunnel | mirror-to-cpu | tunnel-gre-keepalive | loopback-detection | rsvp | bfd-learning | mpls-ttl-fail | fwd-to-cpu | ptp |)

Parameter	Parameter Description	Parameter Value
bpdud	Reason for BPDU protocols packets(including STP, RSTP, MSTP)	-
slow-protocol	Reason for slow protocol packets.(including EFM, LACP)	-
eapol	Reason for Dot1x protocol packets	-
erps	Reason for ERPS protocol packets	-
arp	Reason for ARP protocol packets	-
dhcp	Reason for DHCP protocol packets	-
rip	Reason for RIP protocol packets	-
bgp	Reason for BGP protocol packets	-
ldp	Reason for LDP protocol packets	-
ospf	Reason for OSPF protocol packets	-
pim	Reason for PIM protocol packets	-
vrrp	Reason for VRRP protocol packets	-
ssh	Reason for SSH protocol packets	-
telnet	Reason for Telnet protocol packets	-
mlag	Reason for MLAG protocol packets	-

Parameter	Parameter Description	Parameter Value
tcp	Reason for TCP protocol packets	-
ipda	Reason for packets with IPDA destination to router itself	-
icmp-redirect	Reason for redirecting ICMP	-
learning-full	Reason for learning cache is full	-
mcast_rpf_fail	Reason for multi-cast packets with rpf fail	-
macsa-mismatch	Reason for packets that are discarded for source mac is learned from another security port	-
port-security-discard	Reason for packets that are discarded for fdb number equals to allowed maximum number of security port	-
vlan-security-discard	Reason for packets that are discarded for fdb number equals to allowed maximum number on the specified vlan	-
ip-mtu-fail	Ip mtu fail	-
ip-option	Reason for IP packets with optional fields	-
ucast-ttl-fail	Reason for ucast ip packets with fail TTL	-
mpls-ttl-fail	Reason for mpls packets with fail TTL	-
lgmp	Reason for IGMP or igmp snooping packets	-
sflow-ingress	Reason for sflow sampled packets at ingress direction	-
sflow-egress	Reason for sflow sampled packets at egress direction	-
fwd-to-cpu	Reason for packets forwarding to cpu	-
bfd-learning	Reason for bfd learning packets	-
mld	mld packets or mld snooping packets	-
dot1x-mac-bypass	mac auth bypass packets	-

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This example shows how to show cpu receive BPDU packets:

```
Switch# show cpu traffic-statistics receive bpdu
```

```
statistics rate time is 5 second(s)
```

reason	count(packets)	rate(pps)
bpdu	0	0

Related Commands

```
show cpu traffic-statistics receive all
```

13.3.4 show cpu traffic-statistics receive all**Command Purpose**

Use this command to show CPU receive all packets.

Command Syntax

```
show cpu traffic-statistics receive all
```

Command Mode

Privileged EXEC

Default

N/A

Usage

N/A

Examples

This example shows how to show CPU receive all packets:

```
Switch# show cpu traffic-statistics receive all
```

```
statistics rate time is 5 second(s)
```

reason	count(packets)	rate(pps)
dot1x-mac-bypass	0	0
bpdu	0	0
slow-protocol	0	0
eapol	0	0
erps	0	0
smart-link	0	0
udld	0	0
loopback-detection	0	0
arp	0	0
dhcp	0	0
rip	0	0
ldp	0	0
ospf	0	0
pim	0	0
bgp	0	0
vrrp	0	0
rsvp	0	0
ssh	0	0
telnet	0	0
mlag	0	0
tcp	0	0
ipda	0	0
icmp-redirect	0	0
mcast-rpf-fail	0	0
macsa-mismatch	0	0
port-security-discard	0	0
vlan-security-discard	0	0
ip-mtu-fail	0	0
bfd-learning	0	0
ptp	0	0
ip-option	0	0
tunnel-gre-keepalive	0	0
ucast-ttl-fail	0	0
mpls-ttl-fail	0	0
igmp	0	0
sflow-ingress	0	0
sflow-egress	0	0

fwd-to-cpu	0	0
l2protocol-tunnel	0	0
mirror-to-cpu	0	0
mpls-tp-pwoam	0	0
other	0	0
Total	0	0

Related Commands

N/A

13.3.5 show cpu traffic-statistics transmit

Command Purpose

Use this command to show the CPU transmit all packets.

Command Syntax

```
show cpu-traffic -statistic transmit
```

Command Mode

Privileged EXEC

Default

N/A

Usage

CPU transmit packets statistics not distinguish reason.

Examples

This example shows how to show the CPU transmit all packets:

```
Switch# show cpu traffic-statistics transmit
```

statistics rate time is 5 second(s)

	count(packets)	rate(pps)
Total	0	0

Related Commands

N/A

13.4 CPU Traffic Protect Commands

13.4.1 cpu-traffic-protect

Command Purpose

Use this command to enable and enter into cpu traffic protect mode. Use the no form of this command to disable cpu traffic protect mode.

Command Syntax

cpu-traffic-protect (arp | dhcp)

no cpu-traffic-protect (arp | dhcp)

Parameter	Parameter Description	Parameter Value
arp	ARP packet	-
dhcp	DHCP packet, cpu traffic protect dhcp at port level is enabled.	-

Command Mode

Global Configuration

Default

None

Usage

When `cpu-traffic-protect arp` is configured, blacklist mode is entered default. When `cpu-traffic-protect dhcp` is configured, cpu traffic protect dhcp at port level is enabled.

Examples

This example shows how to enable and enter into cpu traffic protect mode:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)#
```

Related Commands

N/A

13.4.2 trace enable

Command Purpose

Use this command to enable attack trace. Use the no form of this command to disable attack trace.

Command Syntax

trace enable
no trace enable

Command Mode

Cpu traffic Protect Configuration

Default

None

Usage

None

Examples

This example shows how to enable attack trace:

```
Switch# configure terminal  
Switch(config-cpu-traffic-protect)# trace enable
```

Related Commands

N/A

13.4.3 trace type

Command Purpose

Use this command to configure attack trace type. Use the no form of this command to set to the default type.

Command Syntax

trace type (sender-ip | src-mac | target-ip | source-portvlan | src-interface)
no trace type

Parameter	Parameter Description	Parameter Value
sender-ip	ARP packet sender ip address	-
src-mac	ARP packet source MAC	-
target-ip	ARP packet target ip address	-
source-portvlan	The port and vlan packet input	-

Parameter	Parameter Description	Parameter Value
source-interface	The source interface DHCP packet input, only can be used when cpu-traffic-protect dhcp.	-

Command Mode

Cpu traffic Protect Configuration

Default

Trace type default for ARP: src-mac;

Trace type default for DHCP: src-interface

Usage

Trace type of dhcp only supports src-interface, and arp trace type includes all except src-interface.

Examples

This example shows how to configure attack trace type to sender-ip and target-ip:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# trace type sender-ip target-ip
```

Related Commands

N/A

13.4.4 trace sample

Command Purpose

Use this command to configure attack trace sample rate. Use the no form of this command to set sample to the default.

Command Syntax

trace sample SAMPLE-RATE

no trace sample

Parameter	Parameter Description	Parameter Value
SAMPLE-RATE	Attack trace sample rate	1-1024

Command Mode

Cpu traffic Protect Configuration

Default

Trace sample default for ARP: 8;
Trace sample default for DHCP: 1

Usage

None

Examples

This example shows how to configure attack trace sample rate to 16:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# trace sample 16
```

Related Commands

None

13.4.5 trace threshold

Command Purpose

Use this command to configure attack trace checking threshold. Use the no form of this command to set threshold to the default.

Command Syntax

trace threshold THRESHOLD
no trace threshold

Parameter	Parameter Description	Parameter Value
THRESHOLD	Attack trace checking threshold	1-65535,unit:pps

Command Mode

Cpu traffic Protect Configuration

Default

Trace threshold default for ARP: 128;
Trace threshold default for DHCP: 64

Usage

None

Examples

This example shows how to configure attack trace cheking threshold to 10:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# trace threshold 10
```

Related Commands

None

13.4.6 trace timeout

Command Purpose

Use this command to configure trace aging timeout.Use the no form of this command to set aging timeout to the default.

Command Syntax

trace timeout AGING-TIMEOUT

no trace timeout

Parameter	Parameter Description	Parameter Value
AGING-TIMEOUT	Attack trace aging timeout	30-1000000,unit:s

Command Mode

Cpu traiffic Protect Configuration

Default

Trace timeout default for ARP: 300s

Usage

None

Examples

This example shows how to configure attack trace timeout to 400:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# trace timeout 400
```

Related Commands

None

13.4.7 trace action

Command Purpose

Use this command to configure attack trace punish action. Use the no form of this command to set trace action to the default.

Command Syntax

```
trace action deny ( recover time RECOVER-TIME | )
```

```
no trace action
```

Parameter	Parameter Description	Parameter Value
RECOVER-TIME	Attack trace punish action auto-recover time	1-86400,unit:s

Command Mode

Cpu traffic Protect Configuration

Default

recover time 300

Usage

Only used for cpu-traffic-protect dhcp, default is to deny dhcp packets and recover in 300s

Examples

This example shows how to configure attack trace action recover time to 600:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect dhcp
Switch(config-cpu-traffic-protect)# trace action deny recover time 600
```

Related Commands

cpu-traffic-protect manual recover dhcp

13.4.8 trace protect delay-time

Command Purpose

Use this command to configure trace protect delay-time. Use the no form of this command to set protect delay-time to the default.

Command Syntax

```
trace protect delay-time DELAY-TIME
```


no trace delay-time

Parameter	Parameter Description	Parameter Value
DELAY-TIME	delay-time for protect action is enabled	0-86400,unit:s

Command Mode

Cpu traffic Protect Configuration

Default

10

Usage

Only used for cpu-traffic-protect dhcp, represents continuously being attacked for how long time to enable cpu traffic protect dhcp.

Examples

This example shows how to configure attack protect delay-time to 15:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# trace protect delay-time 15
```

Related Commands

None

13.4.9 apply access-list

Command Purpose

Use this command to configure arp protect filter rules. Use the no form of this command to disable rules.

Command Syntax

apply access-list NAME (mode (blacklist | whitelist (rate RATE |)))

no apply access-list ACL-NAME

Parameter	Parameter Description	Parameter Value
ACL-NAME	Extend ip access list name	-
blacklist	Blacklist mode	-
whitelist	Whitelist mode	-
RATE	Packet to cpu rate	32-2048,unit:pps

Command Mode

Cpu traffic Protect Configuration

Default

Rate: 32pps, Mode: blacklist

Usage

The rate is calculated by using 64 Bytes packet

Examples

This example shows how to configure arp protect filter rules with access list 2 and enter into whitelist mode and the rate is 64pps:

```
Switch# configure terminal
Switch(config)# cpu-traffic-protect arp
Switch(config-cpu-traffic-protect)# apply access-list 2 mode whitelist rate 64
```

Related Commands

None

13.4.10 cpu-traffic-protect manual recover dhcp

Command Purpose

Use this command to manually recover dhcp protocol of interfaces being punished by cpu traffic protect.

Command Syntax

cpu-traffic-protect manual recover dhcp (interface (IFPHYSICAL | IFAGG | IFVLAN) | all)

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-
IFVLAN	VLAN interface name	-
all	All interfaces being punished	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to configure cpu-traffic-protect manual recover dhcp for interface eth-0-1:

```
Switch# cpu-traffic-protect manual recover dhcp interface eth-0-1
```

Related Commands

trace action

13.4.11 show cpu traffic-protect dhcp recover table

Command Purpose

Use this command to show the information table of interfaces being protected by cpu traffic and their recover time of dhcp protocol.

Command Syntax

```
show cpu traffic-protect dhcp recover table
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show cpu traffic-protect dhcp recover table:

```
Switch# show cpu traffic-protect dhcp recover table
```

Dhcp Recover State Table :

Interface	RecoverTime(s)
eth-0-1	30
Total: 1	

Related Commands

trace protect delay-time

13.4.12 show cpu traffic-protect trace

Command Purpose

Use this command to show the information of attack trace.

Command Syntax

show cpu traffic-protect (arp | dhcp) trace (history |)

Parameter	Parameter Description	Parameter Value
arp	ARP packet	-
dhcp	DHCP packet	-
history	History trace information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of arp attack trace:

```
Switch# show cpu traffic-protect arp trace
```

Attack Source User Table :

MacAddress	Interface	Vlan:O/I	AttackTime	TotalPackets
0000.0b00.0200	eth-0-3	-	2019-01-02 15:18:21	1712

Total: 1

Attack Source Port Table :

Interface	Vlan:O/I	AttackTime	TotalPackets

Total: 0

Attack Sender IP Table :

IPAddress	AttackTime	TotalPackets
1.2.3.4	2019-01-02 15:21:24	184

Total: 1

Attack Target IP Table :

IPAddress	AttackTime	TotalPackets
4.3.2.1	2019-01-02 15:21:24	184

Total: 1

Related Commands

clear cpu traffic-protect trace

13.4.13 show cpu traffic-protect trace config

Command Purpose

Use this command to show the configure information of attack trace config.

Command Syntax

show cpu traffic-protect (arp | dhcp) trace config

Parameter	Parameter Description	Parameter Value
arp	ARP packet	-
dhcp	DHCP packet	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of arp attack trace config:

```
Switch# show cpu traffic-protect arp trace config
```

Trace arp configuration:

```
Reason          :16
Enable          :1
Mode            :0x1
Sample          :18
Threshold       :35
Aging timeout   :300
```

Related Commands

None

13.4.14 clear cpu traffic-protect trace

Command Purpose

Use this command to clear the history information of attack trace.

Command Syntax

```
clear cpu traffic-protect ( arp | dhcp ) trace ( history | )
```

Parameter	Parameter Description	Parameter Value
arp	ARP packet	-
dhcp	DHCP packet	-
history	History trace information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear the information of arp attack history trace:

```
Switch# clear cpu traffic-protect arp trace history
```

Related Commands

None

13.5 UDLD Commands

13.5.1 udd enable

Command Purpose

Use this command enable/disable global UDLD state.

Command Syntax

udd enable
no udd enable

Command Mode

Global Configuration

Default

Disabled

Usage

None

Examples

This example shows how to enable global UDLD state:

```
Switch# configure terminal  
Switch(config)# udd enable
```

Related Commands

show udd

13.5.2 udd port

Command Purpose

Use this command to enable/disable UDLD state on a specific interface.

Command Syntax

udd port (aggressive |)

no udd port

Parameter	Parameter Description	Parameter Value
aggressive	UDLD aggressive mode	-

Command Mode

Interface Configuration

Default

Disabled

Usage

None

Examples

This example shows how to enable UDLD on interface eth-0-9:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config)# udd port
```

Related Commands

show udd

13.5.3 udd message interval

Command Purpose

Use this command to set the UDLD message interval. Use no command to set the interval to default value.

Command Syntax

udd message interval *INTERVAL*

no udd message interval

Parameter	Parameter Description	Parameter Value
INTERVAL	UDLD message interval (seconds). The range is 1-90	1-90 seconds

Command Mode

Global Configuration

Default

15s

Usage

None

Examples

This example shows how to set UDLD message interval to 5 seconds:

```
Switch# configure terminal
```

```
Switch(config)# udld message interval 5
```

Related Commands

show udld

13.5.4 udld reset**Command Purpose**

Use this command to reset the interfaces disabled by UDLD.

Command Syntax

udld reset

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to reset interfaces disabled by UDLD:

```
Switch# udld reset
```

Related Commands

None

13.5.5 show udld**Command Purpose**

Use this command to show UDLD information of interfaces.

Command Syntax

```
show udld ( IFNAME | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	Interface name	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show UDLD information of interface eth-0-1:

```
Switch# show udld eth-0-1
```

```
Interface eth-0-1
```

```
----
```

```
UDLD mode      : aggressive mode
```

```
Operational state : Bidirectional
```

```
Message interval : 15
Time out interval : 3
Neighbor 1
---
Device ID       : 001e.0808.0360
Port ID        : eth-0-2
Device Name     : DUT2
Message Interval : 15
Timeout Interval : 3
Link status     : Bidirectional
Expiration time : 40
```

Related Commands

None

13.5.6 show udlld neighbors

Command Purpose

Use this command to show information of UDLD neighbors.

Command Syntax

```
show udlld neighbors
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show UDLD neighbor information:

```
Switch# show udlld neighbor
```

Port	Device Name	Device ID	Port ID	Neighbor State
eth-0-9	DUT2	d4f2.489f.d100	eth-0-9	bidirectional

Related Commands

None

13.5.7 debug udd

Command Purpose

Use this command to debug UDL.

Command Syntax

debug udd (all | packet | events)

no debug udd (all | packet | events)

Parameter	Parameter Description	Parameter Value
all	Show both packet and events	-
packet	Show packets only	-
events	Show events only	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to enable UDL debug for packets:

```
Switch# debug udd packet
```

Related Commands

None

13.5.8 show debugging udd

Command Purpose

Use this command to show UDLD debugging status.

Command Syntax

```
show debugging udld
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show UDLD debugging status:

```
Switch# show debugging udld
```

Related Commands

None

13.6 ERPS Commands

13.6.1 Erps

Command Purpose

Use this command to create erps domain instance.

Use the no form of this command to remove the erps domain instance

Command Syntax

```
erps DOMAINID ( ERPS_NAME | )
```

```
no erps DOMAINID
```

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID.	1-255
ERPS_NAME	ERPS domain name	String with up to 15 characters

Command Mode

Global Configuration

Default

None

Usage

This command is used to create or delete an erps domain. The command should be used first when configuring erps.

ERPS_NAME is optional. If no name is provided by command, system will generate the domain name automatically. The name format follows "ERPS001", where 001 can be instead of any domain ID between 1-255 provided through the command.

Examples

This example shows how to create an erps domain with ID 11 and name test11:

```
Switch# configure terminal
Switch(config)# erps 11 test11
```

Related Commands

show erps list

13.6.2 erps control vlan

Command Purpose

Use this command to specify erps domain's control vlan.

Use the no form of this command to remove the control vlan.

Command Syntax

erps *DOMAINID* (primary | sub) control vlan *VLANID*

no erps *DOMAINID* (primary | sub) control vlan

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID.	1-255
primary	primary ring	-
sub	sub ring	-
VLANID	vlan id	2-4094

Command Mode

Global Configuration

Default

None

Usage

The erps protocol packet is transferred in the control vlan.

It is best to add the control vlan into the instance which is bound by the domain.

Examples

This example shows how to set vlan 15 as primary control vlan for erps domain 11:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 15
Switch(config-vlan)# exit
Switch(config)# erps 11 primary control vlan 15
```

Related Commands

show erps

13.6.3 erps hellotime

Command Purpose

Use this command to set hello timer interval for specific erps domain instance.

Use the no form of this command to restore the default value.

Command Syntax

erps *DOMAINID* hellotime *HELLOTIME*

no erps *DOMAINID* hellotime

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID.	1-255
HELLOTIME	Hello timer interval	1-150 in the multiple of 100 ms

Command Mode

Global Configuration

Default

The default hellotime is 10 (1 second) , unit is 100ms

Usage

The timer should be the same of all nodes in the ring.

Examples

This example shows how to set hello timer interval of erps domain 11 to 20s:

```
Switch# configure terminal
Switch(config)# erps 11 hellotime 20
```

Related Commands

show erps

13.6.4 erps failtime

Command Purpose

Use this command to set the fail timer interval for specific erps domain instance.

Use the no form of this command to restore the default value.

Command Syntax

erps *DOMAINID* failtime *FAILTIME*

no erps *DOMAINID* failtime

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID.	1-255
FAILTIME	Fail timer interval	3-450 in the multiple of 100 ms

Command Mode

Global Configuration

Default

The default failtime is 30(3 seconds), unit is 100ms

Usage

The timer should be the same of all nodes in the ring.

Examples

This example shows how to set fail timer interval of erps domain 11 to 60s:


```
Switch# configure terminal
Switch(config)# erps 11 failtime 60
```

Related Commands

show erps

13.6.5 erps mstp instance

Command Purpose

Use this command to set the mstp instance protected by ERPS.

Use the no form of this command to remove the protected mstp instance.

Command Syntax

erps *DOMAINID* mstp instance *INSTANCE_ID*

no erps *DOMAINID* mstp instanc

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
INSTANCE_ID	MSTP instance.	1-4094

Command Mode

Global Configuration

Default

None

Usage

No default instance is specified.

Examples

This example shows how to set instance 1 as ERPS11's protected instance:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# erps 11 mstp instance 1
```

Related Commands

show erps

13.6.6 erps ring level

Command Purpose

Use this command to create an ERPS ring for specific ERPS domain.

Use the no form of this command to remove the ERPS ring.

Command Syntax

erps *DOMAINID* ring *RINGID* level (primary | sub)

no erps *DOMAINID* ring *RINGID*

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
primary	Primary ring	-
sub	Sub ring	-

Command Mode

Global Configuration

Default

None

Usage

The rings in the erps domain are divided into primary and subrings that are differentiated by the configuration.

Examples

This example shows how to create a sub ring with ID 1 for ERPS domain 11:

```
Switch# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#erps 11 ring 1 level sub
```

Related Commands

```
show erps
```

13.6.7 erps ring mode

Command Purpose

Use this command to set specific ERPS ring instance node mode.

Use the no form of this command to restore the default mode.

Command Syntax

erps *DOMAINID* ring *RINGID* mode (master | transit | vpls)

no erps *DOMAINID* ring *RINGID* mode

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
master	Master node	-
transit	Transit node	-
vpls	VPLS node	-

Command Mode

Global Configuration

Default

The mode is not set by default.

Usage

The master node is used to send and receive erps protocol packet.

The transit and vpls node is used to transfer erps protocol packet to neighbor switch.

Examples

This example shows how to set node as ERPS domain 11 ring 1 transit node:

```
Switch# configure terminal
```

```
Switch(config)# erps 11 ring 1 mode transit
```

Related Commands

show erps

13.6.8 erps ring primary interface

Command Purpose

Use this command to set primary interface for specific ERPS ring instance.

Use the no form of this command to unset the primary interface.

Command Syntax

erps *DOMAINID* ring *RINGID* primary interface (*IFPHYSICAL* | *IFAGG*)

no erps *DOMAINID* ring *RINGID* primary interface

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Global Configuration

Default

None

Usage

For master node, the interface with type primary is used to send erps protocol packet.

Only the interface in trunk/dot1q-tunnel mode can be set as primary interface.

Examples

This example shows how to set interface eth-0-9 as primary interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#interface eth-0-9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 15
Switch(config-if)#exit
Switch(config)#erps 11 ring 1 primary interface eth-0-9
```

Related Commands

show erps

13.6.9 erps ring secondary interface

Command Purpose

Use this command to set secondary interface for specific ERPS ring instance.

Use the no form of this command to unset the secondary interface.

Command Syntax

erps *DOMAINID* ring *RINGID* secondary interface (*IFPHYSICAL* | *IFAGG*)

no erps *DOMAINID* ring *RINGID* secondary interface

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Global Configuration

Default

None

Usage

Only the interface in trunk/dot1q-tunnel mode can be set as secondary interface.

Examples

This example shows how to set interface eth-0-9 as primary interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#interface eth-0-9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 15
Switch(config-if)#exit
Switch(config)#erps 11 ring 1 secondary interface eth-0-9
```

Related Commands

show erps

13.6.10 erps ring interface

Command Purpose

Use this command to set vpls interface for specific ERPS ring instance.

Use no form of this command to unset vpls interface for specific ERPS ring instance.

Command Syntax

erps *DOMAINID* ring *DOMAINID* interface (*IFPHYSICAL* | *IFAGG*)

no erps *DOMAINID* ring *DOMAINID* interface

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set interface eth-0-9 as vpls interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#interface eth-0-9
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 15
Switch(config-if)#exit
Switch(config)#erps 11 ring 1 interface eth-0-9
```

Related Commands

show erps

13.6.11 erps ring edge-mode

Command Purpose

Use this command to set specific ERPS ring instance edge node mode.

Use the no form of this command to unset specific ERPS ring instance edge node mode.

Command Syntax

erps *DOMAINID* ring *DOMAINID* edge-mode (edge | assistant-edge)

no erps *DOMAINID* ring *DOMAINID* mode

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
edge	Edge node	-
assistant-edge	Assistant-edge node	-

Command Mode

Global Configuration

Default

None

Usage

Both the edge node and the assistant-edge node are special transit nodes.

Once a node is set to edge/assistant-edge node, it will be set to transit node automatically.

Examples

This example shows how to set node as ERPS domain 11 ring 1 edge node:

```
Switch# configure terminal
Switch(config)# erps 11 ring 1 edge-mode edge
```

Related Commands

show erps

13.6.12 erps ring edge interface

Command Purpose

Use this command to set edge interface for specific ERPS ring instance.

Use the no form of this command to unset the edge interface.

Command Syntax

erps *DOMAINID* ring *DOMAINID* edge interface (*IFPHYSICAL* | *IFAGG*)

no erps *DOMAINID* ring *DOMAINID* edge interface

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Global Configuration

Default

None

Usage

Of the two ports via which the edge node (assistant-edge node) accesses the subring, one is a common port and the other is an edge port. The common port is the port for the edge node (assistant-edge node) to access the primary ring and the subring, while the edge port is the port for the edge node to access the subring only.

This command is only available for edge/assistant-edge node.

Examples

This example shows how to set interface eth-0-9 as edge interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
Switch(config)# erps 11 ring 1 edge interface eth-0-9
```

Related Commands

show erps

13.6.13 erps ring common interface

Command Purpose

Use this command to set common interface for specific ERPS ring instance.

Use the no form of this command to set edge interface for specific ERPS ring instance.

Command Syntax

erps *DOMAINID* ring *RINGID* common interface (*IFPHYSICAL* | *IFAGG*)

no erps *DOMAINID* ring *RINGID* common interface

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Global Configuration

Default

None

Usage

Of the two ports via which the edge node (assistant-edge node) accesses the subring, one is a common port and the other is an edge port. The common port is the port for the edge node (assistant-edge node) to access the primary ring and the subring, while the edge port is the port for the edge node to access the subring only.

This command is only available for edge/assistant-edge node.

Examples

This example shows how to set interface eth-0-9 as edge interface for ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 15
Switch(config-if)# exit
Switch(config)# erps 11 ring 1 common interface eth-0-9
```

Related Commands

show erps

13.6.14 erps ring srpt

Command Purpose

Use this command to enable/disable srpt functionality for specific ERPS ring instance.

Command Syntax

erps *DOMAINID* ring *RINGID* srpt (enable | disable)

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255

Parameter	Parameter Description	Parameter Value
RINGID	ERPS ring ID	1-255
enable	Enable the srpt	-
disable	Disable the srp	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to enable srpt functionality for ERPS domain 11 ring 1:

```
Switch# configure terminal
```

```
Switch(config)# erps 11 ring 1 srpt enable
```

Related Commands

```
show erps
```

13.6.15 erps ring enable**Command Purpose**

Use this command to enable specific erps ring instance.

Command Syntax

```
erps DOMAINID ring RINGID enable
```

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255

Command Mode

Global Configuration

Default

None

Usage

Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

Examples

This example shows how to enable ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)#erps 11 ring 1 enable
```

Related Commands

show erps

13.6.16 erps ring disable

Command Purpose

Use this command to disable specific erps ring instance.

Command Syntax

erps *DOMAINID* ring *RINGID* disable

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255
RINGID	ERPS ring ID	1-255

Command Mode

Global Configuration

Default

None

Usage

Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

Examples

This example shows how to disable ERPS domain 11 ring 1:

```
Switch# configure terminal
Switch(config)# erps 11 ring 1 disable
```

Related Commands

show erps

13.6.17 erps enable

Command Purpose

Use this command to enable specific ERPS domain instance.

Command Syntax

erps *DOMAINID* enable

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255

Command Mode

Global Configuration

Default

None

Usage

Use this command to enable all the ring of the erps domain.

Enable the domain will make all the rings within the domain be enabled. Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state

Examples

This example shows how to enable erps domain 11:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# erps 11 enable
```

Related Commands

show erps

13.6.18 erps disable

Command Purpose

Use this command to disable specific erps domain instance.

Command Syntax

erps *DOMAINID* disable

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255

Command Mode

Global Configuration

Default

None

Usage

Use this command to disable all the ring of the erps domain.

Enable the domain will make all the rings within the domain be enabled. Upon the specific ERPS ring is enabled successfully, the ring state should leave the idle state.

Examples

This example shows how to disable erps domain 11:

```
Switch# configure terminal
Switch(config)# erps 11 disable
```

Related Commands

show erps

13.6.19 erps mode rrpp

Command Purpose

Use this command to compatible with RRPP.

Command Syntax

erps mode rrpp
no erps mode rrpp

Command Mode

Global Configuration

Default

None

Usage

This command to compatible with RRPP.

Examples

This example shows how to compatible with RRPP:

```
Switch# configure terminal  
Switch(config)# erps mode rrpp
```

Related Commands

None

13.6.20 show erps

Command Purpose

Use this command to show the configuration for specific erps domain.

Command Syntax

show erps *DOMAINID*

Parameter	Parameter Description	Parameter Value
DOMAINID	ERPS domain ID	1-255

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the configuration for erps domain 1:

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain mode: normal
ERPS domain primary control VLAN ID: 0
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
```

Related Commands

None

13.6.21 show erps list

Command Purpose

Use this command to show the list of erps domain(s).

Command Syntax

```
show erps list
```

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the erps domain list:

```
Switch# show erps list
```

ERPS Domain List

ID	Name

11	ERPS0011

Related Commands

None

13.6.22 clear erps counters

Command Purpose

Use this command to clear the statistics for all domains or for single domain or for single ring.

Command Syntax

```
clear erps counters ( all | ( domain DOMAINID ( | ring RINGID ) ) )
```

Parameter	Parameter Description	Parameter Value
all	All domain	-
domain <i>DOMAINID</i>	ERPS domain ID	1-255
ring <i>RINGID</i>	ERPS ring ID	1-255

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear all domain statistics:

```
Switch# clear erps counters all
```


Related Commands

None

13.6.23 debug erps

Command Purpose

Use this command to open the debug functions of ERPS.

Command Syntax

debug erps (all | dump | events)

no debug erps (all | dump | events)

Parameter	Parameter Description	Parameter Value
all	all debug information	-
dump	dump debug information	-
events	events debug information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to open all debug functions:

```
Switch# debug erps all
```

Related Commands

None

13.7 Smart-Link Commands

13.7.1 smart-link group

Command Purpose

Use this command to create a smart-link group and enter smart-link group configuration mode. To destroy the smart-link group, used no form of this command.

Command Syntax

smart-link group *GROUP-ID*

no smart-link group (*GROUP-ID* | all)

Parameter	Parameter Description	Parameter Value
GROUP-ID	smart-link group ID	1-16
all	All the smart-link groups have been exist	-

Command Mode

Global Configuration

Default

There is no any smart-link group

Usage

Up to 16 smart-link groups can be created.

Examples

Create a smart-link group with ID 1:

```
Switch# configure terminal
```

```
Switch(config)# smart-link group 1
```

Related Commands

```
show smart-link group
```

13.7.2 smart-link relay enable

Command Purpose

Use this command to enable the switch to relay the smart-link flush packet. To disable relaying the packets, use no form of this command.

Command Syntax

smart-link relay enable
no smart-link relay enable

Command Mode

Global Configuration

Default

Relaying the smart-link flush packet is enabled.

Usage

By default, the smart-link flush packet could be flooded. Use the command, "no smart-link relay enable", to disable the packet flooding to other switches.

Examples

The example shows how to enable smart-link relay:

```
Switch# configure terminal  
Switch(config)# smart-link relay enable
```

The example shows how to disable smart-link relay:

```
Switch# configure terminal  
Switch(config)# no smart-link relay enable
```

Related Commands

None

13.7.3 Interface

Command Purpose

Use this command to set master or slave member interface of the smart-link group. To unset the member, uses the no form of this command.

Command Syntax

```
interface ( IFPHYSICAL | IFAGG ) ( master | slave )  
no interface ( master | slave | all )
```

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	The name of physical interface	-
IFAGG	The name of link-agg interface, like agg1	-

Parameter	Parameter Description	Parameter Value
master	The interface act as master role	-
slave	The interface act as slave role	-

Command Mode

Smart-link Configuration

Default

There is no any interface member in the smart-link group by default.

Usage

Every smart-link group has two member interfaces, master and slave. The interfaces should be physical (i.e. eth-0-1) or aggregator (i.e. agg1) switch interface.

STP must be disabled in the smart-link interfaces first.

Examples

This example shows how to set interfaces eth-0-9 and eth-0-13 as the member interfaces of smart-link group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# smart-link group 1
Switch(config-smlk-group)# interface eth-0-9 master
Switch(config-smlk-group)# interface eth-0-13 slave
Switch(config-smlk-group)# end
```

Display the smart link group just created:

```
Switch# show smart-link group 1
```

Smart-link group 1 information:

The smart-link group was disabled.

```
=====
```

Auto-restore:

state	time	count	Last-time
disabled	60	0	N/A

```
=====
```

Protected instance:

Load balance instance:

=====

```
INTERFACE:
Role      Member      DownCount Last-Down-Time  FlushCount Last-Flush-Time
MASTER eth-0-9      0          N/A              0            N/A
SLAVE  eth-0-13      0          N/A              0            N/A
```

Related Commands

show smart-link group

13.7.4 protected mstp instance

Command Purpose

Use this command to set protected MSTP instance to the smart-link group.

Use the no form of this command to unset protected MSTP instance.

Command Syntax

protected mstp instance *INSTANCE-ID*

no protected mstp instance (all | *INSTANCE-ID*)

Parameter	Parameter Description	Parameter Value
INSTANCE-ID	MSTP instance ID. The range is 0-4094	0-4094
all	All the instance have been exist	-

Command Mode

Smart-link Configuration

Default

There is no protected MSTP instance in the smart-link group by default.

Usage

The smart-link groups only protect these VLANs in the protected MSTP instances. The smart-link group can't be enabled if no protected instance is configured. To protect those VLANs which are not bound with MSTP instance, use the command "protected mstp instance 0".

NOTE: If the MTSP instance is removed, it will be removed from smart-link group at the same time.

Examples

This example shows how to set MSTP instance 0, 10 and 100 to the smart-link group 1:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# protected mstp instance 0
Switch(config-smlk-group)# protected mstp instance 10
Switch(config-smlk-group)# protected mstp instance 100
Switch(config-smlk-group)# end
Switch# show smart-link group 1
```

Smart-link group 1 information:

The smart-link group was disabled.

=====

Auto-restore:

state	time	count	Last-time
disabled	60	0	N/A

=====

Protected instance: 0 100 10

Load balance instance:

=====

INTERFACE:

Role	Member	DownCount	Last-Down-Time	FlushCount	Last-Flush-Time
MASTER	eth-0-9	0	N/A	0	N/A
SLAVE	eth-0-13	0	N/A	0	N/A

Related Commands

show smart-link group

13.7.5 load-balance instance

Command Purpose

Use this command to set load-balancing instance to the smart-link group.

Use this command to unset load-balancing instance.

Command Syntax

load-balance instance *INSTANCE-ID*

no load-balance instance (all | *INSTANCE-ID*)

Parameter	Parameter Description	Parameter Value
INSTANCE-ID	MSTP instance ID. The range is 0-4094	0-4094
all	All the instance have been exist	-

Command Mode

Smart-link Configuration

Default

There is no load-balancing instance in the smart-link group by default.

Usage

Load-balancing instances will be active in the slave interface. If user want to configure load-balancing instances, should before the smart-group is enabled.

Examples

This example shows how to set protected instance 10 as the load-balancing instance:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# load-balance instance 10
```

Related Commands

show smart-link group

13.7.6 restore time

Command Purpose

Use this command to set restore time of the smart-link group.
Use the no form of this command to restore the default value.

Command Syntax

```
restore time RESTORE-TIME
no restore time
```

Parameter	Parameter Description	Parameter Value
RESTORE-TIME	The restore time of the smart-link group	30-1200 seconds

Command Mode

Smart-link Configuration

Default

The default restore time is 60 seconds.

Usage

When the master interface is resumed, the links will not be immediately restored to the master interface, but will be delayed a while. The delay time is called restore time.

Examples

This example shows how to set restore time as 30 seconds in the smart-link group 1:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore time 30
```

Related Commands

show smart-link group

13.7.7 restore enable

Command Purpose

Use this command to enable/disable restoring feature of the smart-link group.

Command Syntax

restore enable
no restore enable

Command Mode

Smart-link Configuration

Default

The restoring feature of the smart-link group is disabled by default.

Usage

When master interface fails, the link will be switched to the slave interface. Then, if master interface is resumed, the link will not be switched back to keep the flow stable by default. If restoring feature is enabled, the link will be switched back.

NOTE: If load-balancing instance is configured, this feature is recommended strongly.

Examples

This example shows how to enable the restoring feature in the smart-link group 1:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# restore enable
```

Related Commands

show smart-link group

13.7.8 flush send

Command Purpose

Use this command to set/unset the flush packet sender in the smart-link group.

Command Syntax

flush send control-vlan *VLAN-ID* password simple *PASSWORD*

no flush send

Parameter	Parameter Description	Parameter Value
VLAN-ID	Flush packet will be sent through this VLAN.	1-4094
PASSWORD	The simple password of the flush packet	String with up to 15 characters

Command Mode

Smart-link Configuration

Default

There is no flush sender in the smart-link group by default.

Usage

Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose.

NOTE: If the control-vlan is not existed in the switch, sending flush packet will fail.

Examples

This example shows how to configure flush sender of the smart-link group 1, control-vlan is 4 and password is "test":

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# flush send control-vlan 4 password simple test
```

Related Commands

show smart-link group
smart-link flush receive

13.7.9 group enable

Command Purpose

Use this command to enable/disable the smart-link group.

Command Syntax

group enable
no group enable

Command Mode

Smart-link Configuration

Default

Smart-link group is disabled by default.

Usage

After interface and protected instance configuration is finished, this command could be used to enable the group.

Examples

This example shows how to enable the smart-link group 1:

```
Switch# configure terminal
Switch(config)# smart-link group 1
Switch(config-smlk-group)# group enable
```

Related Commands

show smart-link group

13.7.10 smart-link flush receive

Command Purpose

Use this command to set/unset the flush packet receiver in the switch interface.

Command Syntax

smart-link flush receive control-vlan *VLAN_ID* password simple *PASSWORD*

no smart-link flush receive

Parameter	Parameter Description	Parameter Value
VLAN_ID	Flush packet will be sent through this VLAN.	1-4094
PASSWORD	The simple password of the flush packet	String with up to 15 characters

Command Mode

Interface Configuration

Default

There is no flush receiver by default.

Usage

The received flush packet should have the same VLAN-ID and password with the sender. Otherwise, the packet will be discarded.

Examples

This example shows how to configure flush receiver in the interface eth-0-9, control-vlan is 4 and password is "test":

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# smart-link flush receive control-vlan 4 password simple test
Switch(config-if)# end
Switch# show smart-link
Relay smart-link flush packet is enabled
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 1.
Group-ID    State      MASTER    SLAVE
1           disabled  N/A       N/A
```

Related Commands

flush send

show smart-link

13.7.11 smart-link tcn enable

Command Purpose

Use this command to enable smart link tcn. To disable the smart-link tcn, used no form of this command.

Command Syntax

smart-link tcn enable
no smart-link tcn enable

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# no smart-link tcn enable
Switch# configure terminal
Switch(config)# smart-link tcn enable
```

Related Commands

show smart-link

13.7.12 smart-link tcn query-count

Command Purpose

Use this command to set smart link tcn query count. To reset the smart-link tcn query count to default value, used no form of this command.

Command Syntax

smart-link tcn query-count *QUERY-COUNT*

no smart-link tcn query-count

Parameter	Parameter Description	Parameter Value
QUERY-COUNT	TCN query count.	1-10

Command Mode

Global Configuration

Default

2

Usage

None

Examples

This example shows how to set smart link tcn query count to 5:

```
Switch# configure terminal
```

```
Switch(config)# smart-link tcn query-count 5
```

Related Commands

show smart-link

13.7.13 smart-link tcn query-interval

Command Purpose

Use this command to set smart link tcn query interval. To reset the smart-link tcn query interval to default value, used no form of this command.

Command Syntax

smart-link tcn query-interval *QUERY-INTERVAL*

no smart-link tcn query-interval

Parameter	Parameter Description	Parameter Value
QUERY-INTERVAL	TCN query interval.	1-255 seconds

Command Mode

Global Configuration

Default

10s

Usage

None

Examples

This example shows how to set smart link tcn query interval to 50:

```
Switch# configure terminal
```

```
Switch(config)# smart-link tcn query-interval 50
```

```
Switch# configure terminal
```

```
Switch(config)# no smart-link tcn query-interval
```

Related Commands

show smart-link

13.7.14 show smart-link

Command Purpose

Use this command to display information of all smart-link groups.

Command Syntax

show smart-link

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display summary information of Smart-link group status, including received flush packet, processed flush packet and current Smart-link group number, etc.

Examples

```
Switch# show smart-link
```

```
Relay smart-link flush packet is enabled
```

```
Smart-link received flush packet number:7
```

```
Smart-link processed flush packet number:0
```

```
Smart link Group Number is 1.
```

Group-ID	State	MASTER	SLAVE
1	enabled	eth-0-1	eth-0-2

Related Commands

None

13.7.15 show smart-link group

Command Purpose

Use this command to display detailed information of all smart-link groups or a specific group.

Command Syntax

```
show smart-link group ( GROUP-ID | )
```

Parameter	Parameter Description	Parameter Value
GROUP-ID	Smart-link group ID	1-16

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display detail information of a specified Smart-link group or all Smart-link groups' status.

Examples

```
Switch# show smart-link group 1
```

Related Commands

None

13.7.16 clear smart-link statistic

Command Purpose

Use this command to clear the statistic of the smart-link groups.

Command Syntax

clear smart-link statistic

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear the statistic of the smart-link groups.

Examples

```
Switch# clear smart-link statistic
```

Related Commands

None

13.7.17 debug smart-link

Command Purpose

Use this command to debug detail information of smart link.

Command Syntax

debug smart-link (all | flush | instance | interface | restore)

Parameter	Parameter Description	Parameter Value
all	All debugging	-
flush	Smart-Link Flush Packet	-
instance	Smart-Link Instance	-
interface	Smart-Link Interface	-
restore	Smart-Link auto-restore	-
mib	SNMP MIBs of Smart-Link	-
trap	SNMP trap of Smart-Link	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug smart-link all
```

Related Commands

None

13.8 Multi-Link Commands

13.8.1 multi-link group

Command Purpose

Use this command to create a multi-link group and enter multi-link group configuration mode. To destroy the multi-link group, used no form of this command.

Command Syntax

multi-link group *GROUP-ID*

no multi-link group (*GROUP-ID* | all)

Parameter	Parameter Description	Parameter Value
GROUP-ID	multi-link group ID	1-16

Parameter	Parameter Description	Parameter Value
all	All the multi-link groups have been exist	-

Command Mode

Global Configuration

Default

There is no any multi-link group

Usage

Up to 16 multi-link groups can be created.

Examples

Create a multi-link group with ID 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
```

Related Commands

show multi-link group

13.8.2 multi-link relay enable

Command Purpose

Use this command to enable the switch to relay the multi-link flush packet. To disable relaying the packets, use no form of this command.

Command Syntax

multi-link relay enable
no multi-link relay enable

Command Mode

Global Configuration

Default

Relaying the multi-link flush packet is enabled.

Usage

By default, the multi-link flush packet could be flooded. Use the command, "no multi-link relay enable", to disable the packet flooding to other switches.

Examples

The example shows how to enable multi-link relay:

```
Switch# configure terminal
```

```
Switch(config)# multi-link relay enable
```

The example shows how to disable multi-link relay:

```
Switch# configure terminal
```

```
Switch(config)# no multi-link relay enable
```

Related Commands

None

13.8.3 Interface

Command Purpose

Use this command to set master or slave member interface of the multi-link group. To unset the member uses the no form of this command.

Command Syntax

interface (*IFPHYSICAL* | *IFAGG*) priority <1-4>

no interface (priority <1-4> | all)

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	The name of physical interface, like eth-0-1	-
IFAGG	The name of link-agg interface, like agg1	-
<1-4>	The priority of the interface	1-4
all	Both of the master and slave interface	-

Command Mode

Multi-link Group Configuration

Default

There is no any interface member in the multi-link group by default.

Usage

Every multi-link group has more than two member interfaces. The interfaces should be physical (i.e. eth-0-1) or aggregator (i.e. agg1) switch interface.

NOTE: STP must be disabled in the multi-link interfaces first.

Examples

This example shows how to set interfaces eth-0-9 and eth-0-13 as the interfaces of multi-link group 1:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# interface eth-0-13
Switch(config-if)# spanning-tree port disable
Switch(config-if)# exit
Switch(config)# multi-link group 1
Switch(config-multilink-group)# interface eth-0-9 master
Switch(config-multilink-group)# interface eth-0-13 slave
Switch(config-multilink-group)# end
Switch# show multi-link group 1
```

Multi-link group 1 information:

The multi-link group was disabled.

=====

Auto-restore:

state	time	count	Last-time
disabled	60	0	N/A

=====

Protected instance:

Load balance instance:

=====

INTERFACE:

Role	Member	DownCount	Last-Down-Time	FlushCount	Last-Flush-Time
MASTER	eth-0-9	0	N/A	0	N/A
SLAVE	eth-0-13	0	N/A	0	N/A

Related Commands

show multi-link group

13.8.4 protected mstp instance

Command Purpose

Use this command to set/unset protected MSTP instance to the multi-link group.

Command Syntax

protected mstp instance *INSTANCE-ID*

no protected mstp instance (all | *INSTANCE-ID*)

Parameter	Parameter Description	Parameter Value
INSTANCE-ID	MSTP instance ID. The range is 0-4094	0-4094
all	All the instance have been exist	-

Command Mode

Multi-link Group Configuration

Default

There is no protected MSTP instance in the multi-link group by default.

Usage

The multi-link groups only protect these VLANs in the protected MSTP instances. The multi-link group can't be enabled if no protected instance is configured. To protect those VLANs which are not bound with MSTP instance, use the command "protected mstp instance 0".

NOTE: If the MTSP instance is removed, it will be removed from multi-link group at the same time.

Examples

This example shows how to set MSTP instance 0, 10 and 100 to the multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# protected mstp instance 0
Switch(config-multilink-group)# protected mstp instance 10
Switch(config-multilink-group)# protected mstp instance 100
Switch(config-multilink-group)# end
Switch# show multi-link group 1
```

Multi-link group 1 information:

The multi-link group was enabled.

=====

Auto-restore:

state	time	count	Last-time
disabled	60	0	N/A

```
=====
Protected instance: 0  10  100
```

```
Load balance instance:
```

```
=====
INTERFACE:
```

Role	Member	DownCount	Last-Down-Time	FlushCount	Last-Flush-Time
PRI1	eth-0-9	0	N/A	0	N/A
PRI2	eth-0-10	0	N/A	0	N/A
PRI3	N/A	0	N/A	0	N/A
PRI4	eth-0-12	0	N/A	0	N/A

```
=====
```

```
Instance states in the member interfaces:
```

```
  A - ACTIVE,   B -BLOCK  , D-The interface is link-down
```

Map-instance-ID	P1(eth-0-9)	P2(eth-0-10)	P3(N/A)	P4(eth-0-12)
0	A	B	D	B
10	A	B	D	B
100	A	B	D	B

Related Commands

show multi-link group

13.8.5 load-balance instance

Command Purpose

Use this command to set/unset load-balancing to the multi-link group.

Command Syntax

load-balance instance *INSTANCE-ID* priority <2-4>

no load-balance instance (all | *INSTANCE-ID*)

Parameter	Parameter Description	Parameter Value
INSTANCE-ID	MSTP instance ID. The range is 0-4094	0-4094
<2-4>	Set load-balancing port with same priority	-
all	All the instance have been exist	-

Command Mode

Multi-link Group Configuration

Default

There is no load-balancing instance in the multi-link group by default.

Usage

Load-balancing instances will be active in the slave interface. If user want to configure load-balancing instances, should before the smart-group is enabled.

Examples

This example shows how to set protected instance 10 as the load-balancing instance:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# load-balance instance 10 priority 2
```

Related Commands

show multi-link group

13.8.6 restore time

Command Purpose

Use this command to set restore time of the multi-link group.

Command Syntax

restore time *RESTORE-TIME*

no restore time

Parameter	Parameter Description	Parameter Value
RESTORE-TIME	The restore time of the multi-link group	30-1200 seconds

Command Mode

Multi-link Group Configuration

Default

The default restore time is 60 seconds.

Usage

When the master interface is resumed, the links will not be immediately restored to the master interface, but will be delayed a while. The delay time is called restore time.

Examples

This example shows how to set restore time as 30 seconds in the multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# restore time 30
```

Related Commands

show multi-link group

13.8.7 restore enable

Command Purpose

Use this command to enable/disable restoring feature of the multi-link group.

Command Syntax

```
restore enable
no restore enable
```

Command Mode

Multi-link Group Configuration

Default

The restoring feature of the multi-link group is disabled by default.

Usage

When master interface fails, the link will be switched to the slave interface. Then, if master interface is resumed, the link will not be switched back to keep the flow stable by default. If restoring feature is enabled, the link will be switched back.

NOTE: If load-balancing instance is configured, this feature is recommended strongly.

Examples

This example shows how to enable the restoring feature in the multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# restore enable
```


Related Commands

show multi-link group

13.8.8 flush send

Command Purpose

Use this command to set/unset the flush packet sender in the multi-link group.

Command Syntax

flush send control-vlan *VLAN-ID* password simple *PASSWORD*

no flush send

Parameter	Parameter Description	Parameter Value
VLAN-ID	Flush packet will be sent through this VLAN.	1-4094
PASSWORD	The simple password of the flush packet	String with up to 15 characters

Command Mode

Multi-link Group Configuration

Default

There is no flush sender in the multi-link group by default.

Usage

Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose.

NOTE: If the control-vlan is not existed in the switch, sending flush packet will fail.

Examples

This example shows how to configure flush sender of the multi-link group 1, control-vlan is 4 and password is "test":

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# flush send control-vlan 4 password simple test
```

Related Commands

show multi-link group

multi-link flush receive

13.8.9 group enable

Command Purpose

Use this command to enable/disable the multi-link group.

Command Syntax

group enable
no group enable

Command Mode

Multi-link Group Configuration

Default

Multi-link group is disabled by default.

Usage

After interface and protected instance configuration is finished, this command could be used to enable the group.

Examples

This example shows how to enable the multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# group enable
```

Related Commands

show multi-link group

13.8.10 multi-link flush receive

Command Purpose

Use this command to set/unset the flush packet receiver in the switch interface.

Command Syntax

multi-link flush receive control-vlan *VLAN-ID* password simple *PASSWORD*

no multi-link flush receive

Parameter	Parameter Description	Parameter Value
VLAN-ID	Flush packet will be sent through this VLAN.	1-4094
PASSWORD	The simple password of the flush packet	String with up to 15 characters

Command Mode

Interface Configuration

Default

There is no flush receiver by default.

Usage

The received flush packet should have the same VLAN-ID and password with the sender. Otherwise, the packet will be discarded.

Examples

This example shows how to configure flush receiver in the interface eth-0-9, control-vlan is 4 and password is "test":

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# multi-link flush receive control-vlan 4 password simple test
Switch(config-if)# end
Switch# show multi-link
```

```
Relay multi-link flush packet is enabled
Multi-link received flush packet number:0
Multi-link processed flush packet number:0
Multi-link tcn is enabled
Multi-link tcn query count      :2
Multi-link tcn query interval :3
Multi-link Group Number is 1.
```

Group-ID	State	Pri-1	Pri-2	Pri-3	Pri-4
1	enabled	eth-0-9	eth-0-10	N/A	eth-0-12

Related Commands

flush send

show multi-link

13.8.11 multi-link tcn enable

Command Purpose

Use this command to enable multi-link tcn. To disable the multi-link tcn, used no form of this command.

Command Syntax

multi-link tcn enable
no multi-link tcn enable

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# multi-link tcn enable
Switch# configure terminal
Switch(config)# no multi-link tcn enable
```

Related Commands

show multi-link

13.8.12 multi-link tcn query-count

Command Purpose

Use this command to set multi-link tcn query count. To reset the multi-link tcn query count to default value, used no form of this command.

Command Syntax

multi-link tcn query-count *QUERY-COUNT*
no multi-link tcn query-count

Parameter	Parameter Description	Parameter Value
QUERY-COUNT	TCN query count.	1-10

Command Mode

Global Configuration

Default

2

Usage

None

Examples

This example shows how to set multi-link tcn query count to 5:

```
Switch# configure terminal
Switch(config)# multi-link tcn query-count 5
```

Related Commands

show multi-link

13.8.13 multi-link tcn query-interval**Command Purpose**

Use this command to set multi-link tcn query interval. To reset the multi-link tcn query interval to default value, used no form of this command.

Command Syntax

multi-link tcn query-interval *QUERY-INTERVAL*
no multi-link tcn query-interval

Parameter	Parameter Description	Parameter Value
QUERY-INTERVAL	TCN query interval.	1-255 seconds

Command Mode

Global Configuration

Default

10s

Usage

None

Examples

This example shows how to set multi-link tcn query interval to 50:

```
Switch# configure terminal
```

```
Switch(config)# multi-link tcn query-interval 50
```

This example shows how to restore the default multi-link tcn query interval to 50:

```
Switch# configure terminal
```

```
Switch(config)# no multi-link tcn query-interval
```

Related Commands

show multi-link

13.8.14 show multi-link

Command Purpose

Use this command to display information of all multi-link groups.

Command Syntax

show multi-link

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display a summary information of Multi-link group status, including received flush packet, processed flush packet and current Multi-link group number , etc.

Examples

```
Switch# show multi-link
```

```
Relay multi-link flush packet is enabled
```

```
Multi-link received flush packet number:0
Multi-link processed flush packet number:0
Multi-link tcu is enabled
Multi-link tcu query count      :2
Multi-link tcu query interval :3
Multi-link Group Number is 1.
```

Group-ID	State	Pri-1	Pri-2	Pri-3	Pri-4
1	enabled	eth-0-9	eth-0-10	N/A	eth-0-12

Related Commands

None

13.8.15 show multi-link group

Command Purpose

Use this command to display detailed information of all multi-link groups or a specific group.

Command Syntax

show multi-link group (*GROUP-ID* |)

Parameter	Parameter Description	Parameter Value
GROUP-ID	Multi-link group ID	1-16

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display detail information of a specified Multi-link group or all Multi-link groups' status.

Examples

```
Switch# show multi-link group 1
```

Related Commands

None

13.8.16 clear multi-link statistic

Command Purpose

Use this command to clear the statistic of the multi-link groups.

Command Syntax

clear multi-link statistic

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear the statistic of the multi-link groups.

Examples

```
Switch# clear multi-link statistic
```

Related Commands

None

13.8.17 debug multi-link

Command Purpose

Use this command to debug detail information of multi-link.

Command Syntax

debug multi-link (all | flush | instance | interface | restore)

Parameter	Parameter Description	Parameter Value
all	All debugging	-
flush	Multi-link Flush Packet	-
instance	Multi-link Instance	-
interface	Multi-link Interface	-
restore	Multi-link auto-restore	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# debug multi-link all
```

Related Commands

None

13.8.18 multilink-enhance interface

Command Purpose

Use this command to set/unset the multilink enhance interface which sends enhanced packets in the multi-link group.

Command Syntax

multilink-enhance interface (*IFPHYSICAL* | *IFAGG*)

no multilink-enhance interface

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	The name of physical interface, like eth-0-1	-
IFAGG	The name of link-agg interface, like agg1	-

Command Mode

Multi-link Group Configuration

Default

There is no flush sender in the multi-link group by default.

Usage

The interface of multilink-enhance is generally out of multi-link group, when you want to configure multilink-enhance interface , you should set the control vlan id and password of flush send.

Examples

This example shows how to configure multilink-enhance of multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# multilink-enhance interface eth-0-1
```

Related Commands

show multi-link group

13.8.19 multilink-enhance receive

Command Purpose

Use this command to set/unset the multilink enhance interface which receives enhanced packets in multi-link group.

Command Syntax

multilink-enhance receive control-vlan *VLAN-ID* password simple *PASSWORD* interface (*IFPHYSICAL* | *IFAGG*)

no multilink-enhance receive interface (*IFPHYSICAL* | *IFAGG*)

Parameter	Parameter Description	Parameter Value
control-vlan VLAN-ID	The VLAN ID of multi-link control vlan	1-4094
password simple PASSWORD	The simple password	String with up to 15 characters
IFPHYSICAL	The name of physical interface, like eth-0-1	-
IFAGG	The name of link-agg interface, like agg1	-

Command Mode

Multi-link Group Configuration

Default

There is no flush sender in the multi-link group by default.

Usage

The received interface of multilink-enhance must be the member of multi-link group with the lowest priority. When the interface enabling receiving enhanced packets, it should not be set the load-balance, and doesn't add the lower priority interface in multi-link group.

Examples

This example shows how to configure multilink-enhance received interface of multi-link group 1:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# multilink-enhance receive control-vlan 10 password b interface eth-0-2
```

Related Commands

show multi-link group

13.8.20 multilink-enhance send-interval

Command Purpose

Use this command to set the interval of sending enhance packets.

Command Syntax

multilink-enhance send-interval <1-255>

no multilink-enhance send-interval

Parameter	Parameter Description	Parameter Value
<1-255>	The interval of sending enhance packets	1-255

Command Mode

Multi-link Group Configuration

Default

10

Usage

NONE.

Examples

This example shows how to configure the interval of sending enhance packets, its value is 20:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# multilink-enhance send-interval 20
```

Related Commands

show multi-link group

13.8.21 multilink-enhance timeout

Command Purpose

Use this command to set the interval of checking received enhance packets.

Command Syntax

multilink-enhance timeout <1-255>

no multilink-enhance timeout

Parameter	Parameter Description	Parameter Value
<1-255>	The interval of checking received enhance packets	1-255

Command Mode

Multi-link Group Configuration

Default

10

Usage

NONE.

Examples

This example shows how to configure the interval of checking received enhance packets, its value is 20:

```
Switch# configure terminal
Switch(config)# multi-link group 1
Switch(config-multilink-group)# multilink-enhance timeout 20
```

Related Commands

show multi-link group

13.9 Monitor Link Commands

13.9.1 monitor-link group

Command Purpose

Use this command to create monitor link group.

Command Syntax

monitor link group *GROUP-ID*

no monitor link group *GROUP-ID*

Parameter	Parameter Description	Parameter Value
GROUP-ID	Monitor link group number	1-16

Command Mode

Global Configuration

Default

No monitor link group is created

Usage

This command is used to create monitor link group. The group range is 1-16.

Examples

In the following example, monitor link group 1 is created:

```
Switch# configure terminal
Switch(config)# monitor-link group 1
```

Related Commands

no monitor-link group

13.9.2 monitor-link uplink interface

Command Purpose

Use this command to add uplink interface to monitor link group.

Command Syntax

monitor-link uplink interface (*IFPHYSICAL* | *IFAGG*)

no monitor-link uplink interface (*IFPHYSICAL* | *IFAGG*)

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Monitor-link Configuration

Default

No interface is add

Usage

Only Ethernet interface and aggregation interface can be used as monitor link group.

Examples

In the following example, the ethernet interface is set to monitor link group member:

```
Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink interface eth-0-1
```

Related Commands

show monitor-link group

13.9.3 monitor-link uplink smart-link group

Command Purpose

Use this command to add smart link group to monitor link group.

Command Syntax

monitor-link uplink smart-link group *GROUP-ID*

no monitor-link uplink smart-link group *GROUP-ID*

Parameter	Parameter Description	Parameter Value
GROUP-ID	Monitor link group number	1-16

Command Mode

Monitor-link Configuration

Default

No smart link group is add

Usage

Only the smart link group which is enabled can be add to monitor link group

Examples

In the following example, the smart link group is set to monitor link group member:

```
Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link uplink smart-link group 1
```

Related Commands

show monitor-link group

13.9.4 no monitor-link uplink

Command Purpose

Use this command to delete all the uplink from monitor link group.

Command Syntax

no monitor-link uplink

Command Mode

Monitor-link Configuration

Default

None

Usage

This command is used to delete all the uplink from monitor link group.

Examples

In the following example, all the uplink is deleted from monitor link group:

```
Switch# configure terminal
Switch(config-mtlk-group)# no monitor-link uplink
```

Related Commands

show monitor-link group

13.9.5 monitor-link downlink interface

Command Purpose

Use this command to add downlink interface from monitor link group.

Command Syntax

monitor-link downlink interface (*IFPHYSICAL* | *IFAGG*)

no monitor-link downlink interface (*IFPHYSICAL* | *IFAGG* |)

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	Ethernet interface name	-
IFAGG	Link aggregation interface name	-

Command Mode

Monitor-link Configuration

Default

No interface is add

Usage

Only Ethernet interface and aggregation interface can be add to monitor link group.

Examples

In the following example, the Ethernet interface is set to monitor link group member:

```
Switch# configure terminal
Switch(config)# monitor-link group 1
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-1
```

Related Commands

show monitor-link group

13.9.6 monitor-link recover-time

Command Purpose

Use this command to set recover time for monitor link group.

Command Syntax

monitor-link recover-time *RECOVER_TIME*

no monitor-link recover-time

Parameter	Parameter Description	Parameter Value
RECOVER_TIME	Monitor link group recover time range (second)	0-60 seconds

Command Mode

Global Configuration

Default

The default value is 3 seconds

Usage

This command is used to set recover time for monitor link group. If the uplink is change to up, all the downlink will be set to up after recover timer.

Examples

In the following example, monitor link group's recover-time is set to 1s:

```
Switch# configure terminal
Switch(config)# monitor-link recover-time 1
```

Related Commands

show monitor-link group

13.9.7 show monitor-link group

Command Purpose

Use this command to display all the monitor link group status.

Command Syntax

show monitor-link group (*GROUP-ID* |)

Parameter	Parameter Description	Parameter Value
GROUP-ID	Monitor link group number	1-16

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display a specified or all the monitor link group status, including status, group id, uptime, downtime, etc.

Examples

In the following example, monitor link group 1 is displayed:

```
Switch# show monitor-link group
```

```
Group Id: 1
```

```
Monitor link status: UP
```

Role	Member	Last-up-time	Last-down-time	upcount	downcount
UpLk 1	eth-0-2	2011/07/15,01:34:17	2011/07/15,01:34:14	1	1

Related Commands

None

13.9.8 debug monitor-link

Command Purpose

Use this command to debug monitor link.

Command Syntax

```
debug monitor-link
```

Command Mode

Privileged EXEC

Default

None.

Usage

None.

Examples

In the following example, the debug of monitor link is set to on:

```
Switch# debug monitor-link
```

Related Commands

None

13.10 VRRP Commands**13.10.1 advertisement-interval****Command Purpose**

To configure the interval between successive advertisements sent by the master virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the advertisement-interval command in router configuration mode. To restore the default value, use the no form of this command.

Command Syntax

advertisement-interval interval

no advertisement-interval

Parameter	Parameter Description	Parameter Value
INTERVAL	Time interval between successive advertisements sent by the master virtual router. The unit of the interval is in seconds.	1-255 seconds

Command Mode

Router Configuration

Default

Default is 1 second.

Usage

The advertisements sent by the master virtual router communicate the state and priority of the current master virtual router.

The advertisement-interval command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer value are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer value. If the same timer value is not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.

Examples

The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# advertisement-interval 4
```

Related Commands

advertisement-interval msec

13.10.2 advertisement-interval msec

Command Purpose

To configure the advertisement interval with milli-second mode between successive advertisements sent by the master virtual router in a VRRP group, use the advertisement-interval msec command in router configuration mode. To restore the second mode, use the no form of this command.

Command Syntax

advertisement-interval msec interval

no advertisement-interval msec

Parameter	Parameter Description	Parameter Value
INTERVAL	Time interval between successive advertisements sent by the master virtual router. The unit of the interval is in 100 milli-seconds.	100-900 milli-seconds.

Command Mode

Router Configuration

Default

None

Usage

The advertisements be sent by the master virtual router communicate the state and priority of the current master virtual router.

The advertisement-interval msec command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer values are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer value. If the same timer value is not set, the routers in the VRRP group will not communicate with each other and any misconfigured router will change its state to master.

Examples

The following example shows how to configure the master virtual router to send advertisements every 100 milli-seconds:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# advertisement-interval msec 100
```

Related Commands

advertisement-interval

13.10.3 interface (VRRP)

Command Purpose

To enable the Virtual Router Redundancy Protocol (VRRP) protocol on a specified interface, use the interface command in router mode.

To disable VRRP protocol on this interface, use the no form of this command.

Command Syntax

interface *INTERFACE-ID*

no interface

Parameter	Parameter Description	Parameter Value
INTERFACE-ID	Interface name	-

Command Mode

Router Configuration

Default

None

Usage

The max VRRP group number should be no more than 3 for one VRRP interface.

Examples

The following is a sample output from the interface command:

```
Switch# configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#interface eth-0-1
```

Related Commands

router vrrp

13.10.4 learnmaster-mode

Command Purpose

To enable the backup router to learn advertisement interval from master router, use the learnmaster-mode true command in router mode.
To disable learn advertisement interval from master router, use the learnmaster-mode false command.

Command Syntax

learnmaster-mode (true | false)

Parameter	Parameter Description	Parameter Value
True	Enable learn advertisement interval from master router	-
False	Disable learning advertisement interval from master router	-

Command Mode

Router Configuration

Default

Default is false.

Usage

By default, backup router does not learn advertisement interval from master router.

Examples

The following example shows how to configure a backup router learning advertisement interval from master router.:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# learnmaster-mode true
```

Related Commands

router vrrp

13.10.5 preempt-mode

Command Purpose

To configure the router to take over as master virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current master virtual router, use the preempt-mode enable command in router mode. To disable this function, use the preempt-mode disable command.

Command Syntax

preempt-mode (true | false)

Parameter	Parameter Description	Parameter Value
True	Preemption enabled	-
False	Preemption disabled	-

Command Mode

Router Configuration

Default

Default is true.

Usage

By default, the router configured preempt-mode true will take over as master virtual router for the group if it has a higher priority than the current master virtual router.

Examples

The following example shows how to configure the router to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# preempt-mode true
Switch(config-router)# priority 200
```

Related Commands

preempt delay

13.10.6 priority (VRRP)

Command Purpose

To set the priority level of the router within a Virtual Router Redundancy Protocol (VRRP) group, use the priority command in router configuration mode. To remove the priority level of the router, use the no form of this command.

Command Syntax

priority level

no priority

Parameter	Parameter Description	Parameter Value
level	Priority of the router within the VRRP group. The range is from 1 to 254.	1-254

Command Mode

Router Configuration

Default

Default is 100

Usage

Use this command to control which router becomes the master virtual router.

Examples

The following example shows how to configure the router with a priority of 254:

```
Switch# configure terminal
Switch(config)#router vrrp 1
Switch(config-router)#priority 254
```

Related Commands

router vrrp

13.10.7 router vrrp

Command Purpose

To create a Virtual Router Redundancy Protocol (VRRP) group, use the `router vrrp` command in Global Configuration mode. To remove this VRRP group, use the `no` form of this command.

Command Syntax

`router vrrp GROUP`

`no router vrrp GROUP`

Parameter	Parameter Description	Parameter Value
GROUP	Group number to which the tracking applies	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

The following is a sample shows how to create a VRRP group:

```
Switch# configure terminal
Switch(config)# router vrrp 1
```

Related Commands

None

13.10.8 track (VRRP)

Command Purpose

To configure the Virtual Router Redundancy Protocol (VRRP) to track an object, use the `track` command in router configuration mode. To disable the tracking, use the `no` form of this command.

Command Syntax

`track OBJ_ID ( decrement VALUE )`

`no track`

Parameter	Parameter Description	Parameter Value
OBJ_ID	track object id	1-500

Parameter	Parameter Description	Parameter Value
decrement VALUE	Priority decrement value	1-255

Command Mode

Router Configuration

Default

None

Usage

Use track to monitor an up link interface, so that when the monitoring interface is down, backup can change to master router.
Only 1 track object is valid for one special VRRP group, and the later configured track object will always overwrite the previous one.

Examples

The following is a sample output from the track command:

```
Switch# configure terminal
Switch(config)# track 10 interface eth-0-1 linkstate
Switch(config)# router vrrp 1
Switch(config-router)# track 10
```

Related Commands

router vrrp

13.10.9 enable /disable**Command Purpose**

To enable a VRRP session, use the enable command in router configuration mode.
To disable a VRRP session, use the disable command in router configuration mode.

Command Syntax

enable
disable

Command Mode

Router Configuration

Default

None

Usage

None

Examples

The following is a sample shows how to enable a VRRP session:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# enable
```

The following is a sample shows how to disable a VRRP session:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# disable
```

Related Commands

None

13.10.10 preempt delay

Command Purpose

To configure the master down interval when preempt takes effect.

Command Syntax

preempt delay time

Parameter	Parameter Description	Parameter Value
TIME	Preempt delay time	0-3600 seconds

Command Mode

Router Configuration

Default

Default is 0 second.

Usage

The original master down interval $= (3 \times \text{adv\_interval}) + \text{skew\_time}$. when *preempt delay* time is configured, then master down interval $= (3 \times \text{adv\_interval}) + \text{skew\_time} + \text{preempt\_delay}$. By default, preempt delay is 0 second.

Examples

The following example shows how to configure the router to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router, but delay 30 seconds to preempt:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router)# preempt-mode true
Switch(config-router)# priority 200
Switch(config-router)# preempt delay 30
```

Related Commands

preempt-mode

13.10.11 virtual-ip

Command Purpose

To enable the Virtual Router Redundancy Protocol (VRRP) on an interface and identify the IP address of the virtual router, use the virtual-ip command in router configuration mode. To disable VRRP on the interface and remove the IP address of the virtual router, use the no form of this command.

Command Syntax

virtual-ip *IP-ADDRESS*

no virtual-ip

Parameter	Parameter Description	Parameter Value
IP-ADDRESS	IP address of the virtual router	IPv4 Address

Command Mode

Router Configuration

Default

None

Usage

For VRRP to elect a designated router, at least one router on the cable must have been configured with the primary address of the virtual router.

VRRP does not support address learning. All addresses must be configured.

All routers in the VRRP group must be configured with the same primary address for the virtual router. If different primary addresses are configured, the routers in the VRRP group will not communicate with each other and any mis-configured routers in the group will change their state to master.

The virtual IP address must be in the same subnet with VRRP interface, and if virtual IP is equal to the interface IP address, it is called IP address owner.

Examples

The following example shows how to enable VRRP on eth-0-1. The VRRP group is 1. IP address 10.0.1.20 is the address of the virtual router:

```
Switch# configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.1.1/24
Switch(config)#router vrrp 1
Switch(config-router)#interface eth-0-1
Switch(config-router)#virtual-ip 10.0.1.20
Switch(config-router)#enable
```

Related Commands

router vrrp

13.10.12 show vrrp

Command Purpose

To display a brief or detailed status of one or all configured Virtual Router Redundancy Protocol (VRRP) groups on the router, use the show vrrp command in Privileged EXEC mode.

Command Syntax

show vrrp (group |)

Parameter	Parameter Description	Parameter Value
GROUP	(Optional) Virtual router group number of the group for which information is to be displayed.	1-255

Command Mode

Privileged EXEC

Default

None

Usage

If no group is specified, all groups are displayed.

Examples

The following is a sample output from the show vrrp command:

```
Switch# show vrrp
```

```
VRID <1>
```

```
State           : Master
Virtual IP       : 10.0.20.254(Not IP owner)
Interface        : eth-0-10
VMAC             : 0000.5e00.0101
Advt timer       : 1
Preempt mode     : TRUE
Conf pri         : 200          Run pri   : 200
Master router ip : 10.0.20.1
Master priority  : 200
Master advt timer : 1
Master down timer : 3
Preempt delay    : 100 second(s)
Learn master mode : FALSE
```

Related Commands

```
router vrrp
```

13.10.13 bfd IP_ADDR

Command Purpose

Use this command to enable IP BFD for VRRP under each instance.

Use the "no" form of this command to disable IP BFD for VRRP under each instance.

Command Syntax

```
bfd IP_ADDR { increase PRIORITY }
```

```
no bfd
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	The nexthop address of bfd session	IPv4 Address
PRIORITY	Increase VRRP priority	1-255

Command Mode

VRRP Configuration

Default

By default IP BFD for VRRP is disabled under each VRRP instance.

Usage

Use this command to enable IP BFD for VRRP under each instance.

The IP BFD session should be created after VRRP instance is created and virtual-ip, VRRP interface have both been configured.

The IP BFD session should be destroyed when state of links change to down or VRRP instance is deleted.

Examples

In the following example, IP BFD for VRRP is enabled under the VRRP instance:

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router) # bfd 9.9.9.2
```

In the following example, IP BFD helps VRRP change the running priority other than configured priority when link happen to be down::

```
Switch# configure terminal
Switch(config)# router vrrp 1
Switch(config-router) # bfd 9.9.9.2 increase 30
```

Related Commands

None

13.11 Track Commands

13.11.1 delay up

Command Purpose

Use this command to specify the delay time before communication state of track object changes to up.

Use the no form of this command to restore the default value.

Command Syntax

delay up *SECONDS*

no delay up

Parameter	Parameter Description	Parameter Value
SECONDS	The delay time before the status of track turn up.	1-180 seconds

Command Mode

Track Configuration

Default

By default the delay time is 0.

Usage

None

Examples

In the following example, the delay up command is used to configure delay when object state is turned from down to up:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay up 30
```

Related Commands

delay down

13.11.2 delay down

Command Purpose

Use this command to specify the delay time before communication state of track object changes to down.

Use the no form of this command to restore the default value.

Command Syntax

delay down *SECONDS*

no delay down

Parameter	Parameter Description	Parameter Value
SECONDS	The delay time before the status of track turn down.	1-180 seconds

Command Mode

Track Configuration

Default

By default the delay time is 0.

Usage

None

Examples

In the following example, the delay down command is used to configure delay when object state is turned from up to down:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)# delay down 30
```

Related Commands

delay up

13.11.3 Frequency

Command Purpose

Use this command to set the frequency of IP SLA operation.
Use the no form of this command to restore the default value.

Command Syntax

frequency *SECONDS*
no frequency

Parameter	Parameter Description	Parameter Value
SECONDS	The frequency of IP SLA operation	1-4800 seconds

Command Mode

IP SLA Configuration

Default

The default value is 60 seconds.

Usage

The frequency value should follow this rule:
 $\text{frequency} > \text{interval} * (\text{packets-per-test} - 1) + \text{timeout}$

Examples

In the following example, the frequency command is used to set the rate at which a specified IP SLAs operation repeats:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# frequency 10
```

Related Commands

show ip sla monitor

13.11.4 ip sla monitor

Command Purpose

To create an IP SLA entry and enter IP SLA monitor configuration mode, use ip sla monitor in CONFIG mode.

To delete an IP SLA entry, use the no form of this command.

Command Syntax

```
ip sla monitor ENTRY-NUMBER
no ip sla monitor ENTRY-NUMBER
```

Parameter	Parameter Description	Parameter Value
ENTRY-NUMBER	Identify of ip sla monitor entry	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the ip sla monitor command is used to create an ip sla monitor entry:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)#
```

Related Commands

show ip sla monitor

13.11.5 description string

Command Purpose

To describe the ipsla entry with a string.
Use the no form of this command to delete it.

Command Syntax

description *STRING*

no description

Parameter	Parameter Description	Parameter Value
STRING	description string for IP SLA	String with up to 255 characters

Command Mode

IP SLA Configuration

Default

None

Usage

None

Examples

In the following example shows how to set IP SLA description:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)#description thisisanexampler
```

Related Commands

ip sla monitor schedule

Command Purpose

To enable an IP SLA entry, use ip sla monitor schedule command in CONFIG mode.
To disable an IP SLA entry, use the no form of this command.

Command Syntax

ip sla monitor schedule (*ENTRY-NUMBER*)

Parameter	Parameter Description	Parameter Value
ENTRY-NUMBER	Identify of ip sla monitor entry	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the ip sla monitor schedule command is used to enable an IP SLA monitor entry:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

Related Commands

show ip sla monitor

13.11.6 ip sla monitor schedule**Command Purpose**

To enable an IP SLA entry, use ip sla monitor schedule command in CONFIG mode.

To disable an IP SLA entry, use the no form of this command.

Command Syntax

ip sla monitor schedule (*ENTRY-NUMBER*)

Parameter	Parameter Description	Parameter Value
ENTRY-NUMBER	Identify of ip sla monitor entry	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the ip sla monitor schedule command is used to enable an IP SLA monitor entry:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
Switch(config)# ip sla monitor schedule 1
```

Related Commands

show ip sla monitor

13.11.7 Timeout

Command Purpose

Use this command to set the time value which IP SLA operation wait for the response.

Use the no form of this command to restore the default value.

Command Syntax

timeout *SECONDS*

no timeout

Parameter	Parameter Description	Parameter Value
SECONDS	Time out value	1-4800 seconds

Command Mode

IP SLA Configuration

Default

The default value is 5 seconds.

Usage

The timeout value should follow this rule:

frequency > interval * (packets-per-test - 1) + timeout)

Examples

In the following example, the timeout command is used to set the time range:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# timeout 10
```

Related Commands

show ip sla monitor

13.11.8 Threshold

Command Purpose

Use this command to set the upper threshold value for calculating network monitoring statistics created by an IP SLAs operation. Use the no form of this command to restore the default value.

Command Syntax

```
threshold MILLISECONDS
no threshold
```

Parameter	Parameter Description	Parameter Value
MILLISECONDS	The upper threshold value for calculating network monitoring statistics created by an IP SLAs operation..()	1 - 4800000 milliseconds

Command Mode

IP SLA Configuration

Default

The default value is 5000 milliseconds.

Usage

The threshold value should follow this rule:
timeout ≥ threshold

Examples

In the following example, the threshold command is used to set the threshold time range:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# threshold 10000
```

Related Commands

show ip sla monitor

13.11.9 Interval

Command Purpose

Use this command to set the interval between probe of each ipsla test.

Use the no form of this command to restore the default value

Command Syntax

interval *SECONDS*

no interval

Parameter	Parameter Description	Parameter Value
SECONDS	The interval between probe of each ipsla test	1-4800 seconds

Command Mode

IP SLA Configuration

Default

The default value is 6 seconds.

Usage

The interval value should follow this rule:

(frequency > interval * (packets-per-test - 1) + timeout)

Examples

In the following example, the interval command is used to set the IP SLA interval:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# interval 10
```

Related Commands

show ip sla monitor

13.11.10 Ttl

Command Purpose

Use this command to set the ttl of icmp request send by ipsla test.

Use the no form of this command to restore the default value.

Command Syntax

ttl value

no ttl

Parameter	Parameter Description	Parameter Value
value	TTL value	1-255

Command Mode

IP SLA Configuration

Default

64

Usage

None

Examples

The following example shows how to set TTL for IP SLA:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# ttl 100
```

Related Commands

show ip sla monitor

13.11.11 Tos

Command Purpose

Use this command to set the tos of icmp request send by ipsla test.

Use the no form of this command to restore the default value.

Command Syntax

tos value

no tos

Parameter	Parameter Description	Parameter Value
value	tos value	1-255

Command Mode

IP SLA Configuration

Default

0

Usage

None

Examples

The following example shows how to set tos for IP SLA:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# tos 100
```

Related Commands

show ip sla monitor

13.11.12 data-size

Command Purpose

Use this command to set the protocol data size in the payload of an IP SLAs operation's request packet.

Use the no form of this command to restore the default value.

Command Syntax

data-size *SIZE*

no data-size

Parameter	Parameter Description	Parameter Value
SIZE	The protocol data size in the payload of an IP SLAs operation's request packet	1 - 8100

Command Mode

IP SLA Configuration

Default

28

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-size 100
```

Related Commands

show ip sla monitor

13.11.13 data-pattern**Command Purpose**

Use this command to set the hexadecimal value for data pattern.

Use the no form of this command to restore the default value.

Command Syntax

data-pattern *HEX_STRING*

no data-pattern

Parameter	Parameter Description	Parameter Value
HEX_STRING	Hex string for data patten	0-0xFFFFFFFF

Command Mode

IP SLA Configuration

Default

ABCDABCD

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# data-pattern abababab
```

Related Commands

show ip sla monitor

13.11.14 fail-percent

Command Purpose

Use this command to set the fail percent used to judge test result.
Use the no form of this command to restore the default value.

Command Syntax

fail-percent *PERCENT*
no fail-percent

Parameter	Parameter Description	Parameter Value
PERCENT	The fail percent used to judge test result	1-100

Command Mode

IP SLA Configuration

Default

100

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# fail-percent 100
```

Related Commands

show ip sla monitor

13.11.15 packets-per-test

Command Purpose

Use this command to set the probe count of each test.

Use the no form of this command to restore the default value.

Command Syntax

packets-per-test *NUMBER*

no packets-per-test

Parameter	Parameter Description	Parameter Value
NUMBER	The probe count of each test	1-10

Command Mode

IP SLA Configuration

Default

3

Usage

The packets-per-test value should follow this rule:

$(\text{frequency} > \text{interval} * (\text{packets-per-test} - 1) + \text{timeout})$

Examples

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# packets-per-test 5
```

Related Commands

show ip sla monitor

13.11.16 statistics (packet | test)

Command Purpose

Use this command to set the statistics number of packet and recent test.

Use the no form of this command to restore the default value.

Command Syntax

statistics (packet *PKT_CNT* | test *TEST_CNT*)

no statistics packet

no statistics test

Parameter	Parameter Description	Parameter Value
PKT_CNT	Packet Number for statistic	0-1000
TEST_CNT	The count of test for statistic	1-10

Command Mode

IP SLA Configuration

Default

packet: 50; test: 5

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# statistics packet 60
Switch(config-ipsla)# statistics test 6
```

Related Commands

show ip sla monitor

13.11.17 clear ip sla statistics

Command Purpose

Use this command to clear ipsla statistics.

Command Syntax

clear ip sla statistics *ENTRY_ID*

Parameter	Parameter Description	Parameter Value
ENTRY_ID	IP SLA entry id	1-255

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# clear ip sla statistics 1
```

Related Commands

show ip sla monitor

13.11.18 Track**Command Purpose**

To configure a track object, use the track command in Global Configuration mode.

Command Syntax

track *OBJECT_ID*

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the track command is used to create a track object:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#
```

Related Commands

show track

13.11.19 track interface linkstate

Command Purpose

Use this command to create a track object and track the state of an interface

Command Syntax

track *OBJECT_ID* interface *IFNAME* linkstate

no track *OBJECT_ID*

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500
IFNAME	Interface name	Support physical/aggregation/loopback/vlan/tunnel ports

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the track interface linkstate command is used to create an track object:

```
Switch# configure terminal
Switch(config)# track 1 interface eth-0-1 linkstate
Switch(config-track)#
```

Related Commands

show track

13.11.20 track rtr reachability

Command Purpose

Create a track object and track the state of an ip sla entry, use the track rtr reachability to command in Global Configuration mode. To remove a track, use the no form of this command.

When the state of IP SLA entry is OK or over-threshold, track object state is up; otherwise track object state is down.

Command Syntax

```
track OBJECT_ID rtr ENTRY_ID reachability
no track OBJECT_ID
```

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500
ENTRY_ID	IP SLA entry id	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the track rtr reachability command is used to create a track object:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
```



```
Switch(config-ipsla)# exit
Switch(config)# track 1 rtr 1 reachability
Switch(config-track)#
```

Related Commands

show track

13.11.21 track rtr state

Command Purpose

Create a track object and track the state of an IP SLA entry, use the track rtr state command in Global Configuration mode. To remove a track, use the no form of this command.

When the state of IP SLA entry is OK, track object state is up; otherwise track object state is down.

Command Syntax

```
track OBJECT_ID rtr ENTRY_ID state
no track OBJECT_ID
```

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500
ENTRY_ID	IP SLA entry id	1-255

Command Mode

Global Configuration

Default

None

Usage

None

Examples

In the following example, the track rtr state command is used to create a track object:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# exit
```

```
Switch(config)# track 1 rtr 1 state
Switch(config-track)#
```

Related Commands

show track

13.11.22 track bfd

Command Purpose

Create a track object and track the state of bfd session, use the track bfd command in Global Configuration mode. To remove a track, use the no form of this command.

When the state of bfd session is up, track object state is up; otherwise track object state is down.

Command Syntax

track *OBJECT_ID* bfd source interface *IFNAME* destination *IP_ADDR*

no track *OBJECT_ID*

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500
IFNAME	Interface name	Support physical/aggregation/vlan/ ports
IP_ADDR	Destination IP address of the bfd session	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

The source interface should be a Layer 3 interface and ip address should be configured.

The destination ip address should be in the same network of the interface ip address.

Examples

In the following example, the track bfd command is used to create a track object:

```
Switch# configure terminal
Switch(config)# interface eth-0-9
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# ip address 9.9.9.1/24
Switch(config-if)# quit
Switch(config)# track 1 bfd source interface eth-0-9 destination 9.9.9.2
Switch(config-track)#
```

Related Commands

show track

13.11.23 track bfd session

Command Purpose

Create a track object and track the state of bfd session, use the track bfd session command in Global Configuration mode. To remove a track, use the no form of this command.

When the state of bfd session is up, track object state is up; otherwise track object state is down.

Command Syntax

track *OBJECT_ID* bfd session *SESSION_NAME*

no track *OBJECT_ID*

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500
SESSION_NAME	BFD session name	String with up to 16 characters

Command Mode

Global Configuration

Default

None

Usage

The bfd session should be created before this command configure.

Examples

In the following example, the track bfd session command is used to create a track object:

```
Switch# configure terminal
Switch(config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20
Switch(config)# track 1 bfd session test
Switch(config-track)#
```

Related Commands

show track

13.11.24 type icmp-echo

Command Purpose

Use this command to defines an Echo operation with ICMP packet and enters destination IP address.

Use the no form of this command to delete an Echo operation and destination IP address.

Command Syntax

type icmp-echo *IP_ADDR* (source-interface *IFNAME* |) (source-ip *SRC_IP_ADDR* |)

no type icmp-echo

Parameter	Parameter Description	Parameter Value
IP_ADDR	Destination IP address of sending icmp packet	IPv4 Address
source-interface IFNAME	Source interface of sending icmp packet	Support physical/aggregation/vlan/ ports
SRC_IP_ADDR	Source IP address of sending icmp packet	IPv4 Address

Command Mode

IP SLA Configuration

Default

None

Usage

If the interface specified by source-interface is not one of the out interfaces by routing, packets may not be sent out.

Examples

In the following example, the type echo protocol iplcmpEcho command is used to set ICMP packet and destination IP address:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# type icmp-echo 192.168.0.1
```

Related Commands

show ip sla monitor

13.11.25 show ip sla monitor

Command Purpose

To show IP SLA entries, packet statistics and recent test result, use show ip sla monitor in EXEC mode.

Command Syntax

show ip sla monitor (*ENTRY_ID*) (statistics (packet | test) |)

Parameter	Parameter Description	Parameter Value
ENTRY_ID	Entry number is used to identify ip sla monitor entry, its range is from 1 to 255	1-255

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the show ip sla monitor command is used to show ip sla monitor entries:

```
Switch# show ip sla monitor
```

```
Entry 1
```

```
Type           : Echo
Admin state     : Enable
Destination address : 192.168.0.1
Frequency       : 3 seconds
Timeout        : 2 seconds
Threshold       : 1 seconds
```

```
Running Frequency      : 3 seconds
Vrf                    : vpn1
Return code            : OK
```

Related Commands

ip sla monitor

13.11.26 show track

Command Purpose

To show TRACK entries, use show track in EXEC mode.

Command Syntax

show track *OBJECT_ID*

Parameter	Parameter Description	Parameter Value
OBJECT_ID	Object identity is used to identify track object	1-500

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example, the show track command is used to show track entries:

```
Switch# show track
```

```
Track 2
```

```
Type          : Response Time Reporter(RTR) Reachability
Interface      : eth-0-2
State          : down
Delay up       : 30 seconds
Delay down     : 30 seconds
```

Related Commands

Track

13.11.27 Vrf

Command Purpose

To use IP SLA operations in VPNs, use vrf in ipsla mode. To remove VPN features from IP SLA operations, use the no form of this command.

Command Syntax

vrf *NAME*

no vrf

Parameter	Parameter Description	Parameter Value
NAME	VRF name	String with up to 15 characters

Command Mode

IP SLA Configuration

Default

None

Usage

None

Examples

In the following example, the vrf command is used to use ip sla monitor entry in VPN:

```
Switch# configure terminal
Switch(config)# ip sla monitor 1
Switch(config-ipsla)# vrf vpn1
```

Related Commands

show ip sla monitor

13.12 VARP Commands

13.12.1 ip virtual-router mac

Command Purpose

Use this command to configure a virtual mac for switch.

Use the no form of this command to remove the virtual-router mac.

Command Syntax

ip virtual-router mac mac-addr

no ip virtual-router mac

Parameter	Parameter Description	Parameter Value
mac-addr	Virtual mac address	MAC Address

Command Mode

Global Configuration

Default

None

Usage

This virtual mac is used for interface configured virtual IP address. The address is receive-only; the switch never sends packets with this address as the source. And it only exists in ARP replay for virtual IP.

Examples

The following example is the result of this command:

```
Switch# configure terminal
Switch(config)# ip virtual-router mac 1.1.1
```

Related Commands

ip virtual-router address

13.12.2 ip virtual-router address

Command Purpose

Use this command to configure a virtual IP address for interface.

Use the no form of this command to remove the virtual-router IP.

Command Syntax

ip virtual-router address (*A.B.C.D* | *A.B.C.D/M*)

no ip virtual-router address

Parameter	Parameter Description	Parameter Value
A.B.C.D	Virtual IP address without mask	IPv4 Address
A.B.C.D/M	Virtual IP address with mask	IPv4 Address and mask length

Command Mode

Interface Configuration

Default

None

Usage

The ip virtual-router address command assigns a virtual IP address to the interface . The virtual IP address without mask should be in the subnet of the primary IP address assigned to the interface and the virtual IP address with mask should not be in the subnet of the primary IP address assigned to the interface. The virtual IP address without mask and the virtual IP address with mask must be selected only one to be configured. if virtual mac is not configured, there is no reply to ARP request packet for the virtual IP address.

Examples

The following example is the result of this command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ip virtual-router address 1.1.1.1
```

Related Commands

ip virtual-router mac

13.13 IP BFD Commands

13.13.1 bfd interval

Command Purpose

Use this command to specify the desired transmit interval, receive interval and detect multiplier of IP BFD on the interface.
Use the "no" form of this command to restore the default value.

Command Syntax

`bfd interval { tx MINTX | rx MINRX | multiplier MULTIPLIER }`

`no bfd interval`

Parameter	Parameter Description	Parameter Value
MINTX	Set BFD minimum trasmit interval	3-1000 millisecond
MINRX	Set BFD minimum receive interval	3-1000 millisecond
MULTIPLIER	Set the value of Hello Multiplier	2-15

Command Mode

Interface Configuration

Default

The default value for minimum tx interval and rx interval is 20ms.

The default value for detect multiple is 3.

Usage

Use this command to specify the transmit interval, receive interval and detect multiple of IP BFD on the interface.

This configuration should affect all the IP BFD sessions on this interface. The actual transmit interval and receive interval need to negotiate with another end of the session.

Examples

In the following example, the desired transmit interval is set as 3 ms, the desired receive interval is set as 3 ms, the detect multiplier is set as 3 times:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# bfd interval mintx 3 minrx 3 multiplier 3
```

Related Commands

None

13.13.2 bfd NAME peer-ip A.B.C.D interface

Command Purpose

Use this command to configure one Single-hop IP BFD session.

Use the "no" form of this command to remove the session

Command Syntax

bfd NAME peer-ip A.B.C.D (vrf NAME |) interface (IFPHYSICAL | IFVLAN | IFAGG) (source-ip A.B.C.D |) (auto | local LDISR remote RDISR)
no bfd NAME

Parameter	Parameter Description	Parameter Value
peer-ip A.B.C.D	BFD destination ip address	IPv4 Address
vrf NAME	specify a vrf for bfd	-
interface	specify an interface for single hop bfd	-
Source-ip A.B.C.D	specify source ip address	IPv4 Address
auto	Allocating local discriminator by system	-
LDISR	specify local discriminator by users	1-8191
RDISR	specify local discriminator by users	1-8191

Command Mode

Global Configuration

Default

By default there is no IP Single BFD session to be created.

Usage

Use this command to specify the IP BFD for static route. BFD session is created, the bfd configurations need meet the following conditions:

- The destination ip address should be subnet with the ip address of the binded interface.
- The specified vrf should be same as that of the binded interface. If users don't specify the vrf, the bfd vrf would be default.
- The source ip address should be same as that of the binded interface. If users don't specify the source ip address, the source ip would be got from the binded interface, which is subnet with the destination ip address. If there are many ip addresses of the binded interface subnet the the destination ip address, the primary ip address would be selected firstly, and the smaller values of the ip adderss would be chosen secondly.

If users specify the local and remote discriminator, bfd uses them. Otherwise, the bfd local discriminator would be allocated by system.

Examples

In the following example, the single-hop IP bfd session "test" is created:

```
Switch# configure terminal
```

```
Switch(config)# bfd test peer-ip 9.9.9.2 interface eth-0/9 local 10 remote 20
```

Related Commands

ip route

13.13.3 bfd NAME peer-ip A.B.C.D source-ip

Command Purpose

Use this command to configure one Multi-hop IP BFD session.

Use the "no" form of this command to remove this configuration.

Command Syntax

bfd NAME peer-ip A.B.C.D source-ip A.B.C.D (auto | local LDISR remote RDISR)

no bfd NAME

Parameter	Parameter Description	Parameter Value
NAME	BFD name	String with up to 16 characters
peer-ip A.B.C.D	BFD destination ip address	IPv4 Address
Source-ip A.B.C.D	specify source ip address	IPv4 Address
auto	Allocating local discriminator by system	-
LDISR	specify local discriminator by users	1-8191
RDISR	specify local discriminator by users	1-8191

Command Mode

Global Configuration

Default

By default there is no IP Multiple BFD session to be created.

Usage

Use this command to specify the IP BFD for static route. BFD session is created, the bfd configurations need meet the following conditions:

1.The source ip address should be same as that of the local L3 interface.

If users specify the local and remote discriminator, bfd uses them. Otherwise, the bfd local discriminator would be allocated by system.

Examples

In the following example, the multi-hop IP bfd session "test" is created:

```
Switch# configure terminal
```

```
Switch(config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20
```

Related Commands

ip route

13.13.4 ip route

Command Purpose

Use this command to specify to bind IP BFD session for static route.

Use the "no" form of this command to remove this configuration.

Command Syntax

ip route *PREFIX NEXTHOP* bind bfd *NAME*

no ip route prefix nexthop bind bfd

Parameter	Parameter Description	Parameter Value
PREFIX	IP destination prefix (e.g. 10.0.0.0/8)	IPv4 Address and mask length
NEXTHOP	IP gateway address	-
NAME	bfd session name	String with up to 16 characters

Command Mode

Global Configuration

Default

By default there is no IP BFD session to be binded with one static route.

Usage

Use this command to bind an existent IP BFD session for static route. The session should be create before use this command.

When the ip static route is deleted, the session should be detach from the route, but not destroyed.

Examples

In the following example, the IP bfd session "test" is bound to the static router 1.1.1.0/24 via 9.9.9.2:

```
Switch# configure terminal
```

```
Switch(config)# ip route 1.1.1.0/24 9.9.9.2 bind bfd test
```

Related Commands

ip route

13.13.5 bfd set interval

Command Purpose

Use this command to configure the interval of sending and receiving bfd packets for bfd session.
Use the "no" form of this command to remove this configuration.

Command Syntax

bfd set interval mintx *MINTX* minrx *MINRX* multiplier *MULTIPLIER*

no bfd set interval

Parameter	Parameter Description	Parameter Value
MINTX	The minimum interval of sending bfd packets	3-1000 millisecond
MINRX	The minimum interval of receiving bfd packets	3-1000 millisecond
MULTIPLIER	the times of timeout	2-15

Command Mode

BFD Configuration

Default

By default, the minimum time of sending and receiving packets are respectively 20ms and 20ms, the times of timeout is 3.

Usage

Use this command to specify the mintx, minrx and timeout of bfd session.

Examples

In the following example, set the interval of sending and receiving bfd packets for bfd session "test":

```
Switch# configure terminal
Switch(config)# bfd test
Switch(config-ip-bfd)bfd set interval mintx 30 minrx 30 multiplier 5
```

Related Commands

show bfd session detail

13.13.6 bfd global dscp

Command Purpose

Use this command to configure global dscp value for all multi-hop bfd sessions.
Use the "no" form of this command to remove this configuration.

Command Syntax

bfd set dscp *DSCP*

no bfd global dscp

Parameter	Parameter Description	Parameter Value
DSCP	the dscp value of bfd packet in IP head	0-63

Command Mode

Global Configuration

Default

By default, the dscp value of all the multi-hop bfd sessions is 56.

Usage

Use this command to specify the dscp for all the multi-hop bfd sessions.

Examples

In the following example, user configures to set the global dscp value for all the multi-hop for all the bfd sessions:

```
Switch# configure terminal
Switch(config)# bfd global dscp 63
```

Related Commands

show bfd session detail

13.13.7 bfd set dscp

Command Purpose

Use this command to configure global dscp value for one multi-hop bfd session.

Use the "no" form of this command to remove this configuration.

Command Syntax

bfd set dscp *DSCP*

no bfd set dscp

Parameter	Parameter Description	Parameter Value
DSCP	the dscp value of bfd packet in IP head	0-63

Command Mode

BFD Configuration

Default

By default, the dscp value of one multi-hop bfd sessions is 56.

Usage

Use this command to specify the dscp for one multi-hop bfd session.

When removing this configuration, the dscp of this multiplier bfd session would be the global dscp value when configuring the global dscp.

Examples

In the following example, user configures to set the global dscp value for all the multi-hop for all the bfd sessions:

```
Switch# configure terminal
Switch(config)#bfd test
Switch(config-ip-bfd)# bfd set dscp 63
```

Related Commands

show bfd session detail

13.13.8 show bfd

Command Purpose

Use this command to show the statues of IP BFD module.

Command Syntax

show bfd

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to show the statues of IP BFD module.

Examples

The following example is the result of this command:

```
Switch# show bfd
```

```
BFD ID: 00      Start Time: Thu May  2 03:09:41 2013
```

```
Number of Sessions: 2
```

```
Slow Timer: 1000      Image type: DISTRIBUTED
```

```
Echo Mode: Disabled    BFD Notifications disabled
```

```
Next Session Discriminator: 10
```

```
BFD Clients:
```

```
STATIC -> Client ID: 1
```

```
OSPF -> Client ID: 4
```

Related Commands

None

13.13.9 show bfd static configurations

Command Purpose

Use this command to show the bfd static configurations.

Command Syntax

```
show bfd static configurations ( word | )
```

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to show the bfd static configurations.

Examples

The following example is the result of this command:

```
Switch# show bfd static configurations
```

Name	Type	VRF	LocalDiscr	RemoteDiscr	Src Ip	Dst Ip	interface
Status							
test1	single-hop default		-	-	10.10.10.1	10.10.10.2	vlan10
active							
test2	single-hop test		-	-	9.9.9.1	9.9.9.2	vlan4094
active							
test3	single-hop default		8191	4294967295	10.10.10.1	10.10.10.3	vlan10
active							

Related Commands

None

13.13.10 show bfd session

Command Purpose

Use this command to show the bfd sessions.

Command Syntax

```
show bfd session ( detail | )
```

```
show bfd session SRC DST interface IFNAME ( detail | )
```

```
show bfd session SRC DST ( detail | )
```

```
show bfd session discriminator SESS ( detail | )
```

Parameter	Parameter Description	Parameter Value
detail	Show session details	-
SRC	Local IPv4 address	IPv4 Address
DST	Neighbor IPv4 address	IPv4 Address
IFNAME	BFD Interface	Support physical/aggregation/vlan/ ports
discriminator SESS	BFD session index	1-4294967295

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to show the bfd session.

Use the key word "detail" to show the detailed information.

To filter the show result, user can specify the session's source and destination address and interface.

Examples

The following example is the result of this command :

```
DUT1# show bfd session
```

Abbreviation:

LD: Local Discriminator. RD: Remote Discriminator

S: Single hop session. M: Multi hop session.

SD: Static Discriminator. DD: Dynamic Discriminator

A: Admin down. D:Down. I:Init. U:Up.

```
=====
LD      RD      TYPE ST  UP-Time  Remote-Addr  VRF
8191    4294967295 S-SD D   00:00:00  10.10.10.3   default
8192    0         S-DD D   00:00:00  11.11.11.2   yoush
8193    0         S-DD D   00:00:00  10.10.10.2   default
8194    0         S-DD D   00:00:00  9.9.9.2      test
```

Number of Sessions: 4

```
DUT1# show bfd session detail
```

```
=====
Session Interface : vlan10          Session Name : test3
Lower Layer : IPv4                  Version : 1
Session Type : Single Hop           Session State : Down
Discriminator Type : Static          DSCP : 0
Local Discriminator : 8191           Local Address : 10.10.10.1
Remote Discriminator: 4294967295      Remote Address: 10.10.10.3
Local Port : 49155                  Remote Port : 3784
vrf : default
Diagnostics : None
Timers in Milliseconds :
Min Tx: 20                          Min Rx: 20          Multiplier: 3
Neg Tx: 4                            Neg Rx: 20          Neg detect mult: 3
Sess up time : 00:00:00
Sess down time : 00:00:00
Bind Application : -
```

```
=====
Session Interface : vlan11          Session Name : -
Lower Layer : IPv4                  Version : 1
Session Type : Single Hop           Session State : Down
```

```
Discriminator Type : Dynamic          DSCP : 0
Local Discriminator : 8192            Local Address : 11.11.11.1
Remote Discriminator: 0               Remote Address: 11.11.11.2
Local Port : 49152                   Remote Port : 3784
vrf : yoush
Diagnostics : None
Timers in Milliseconds :
Min Tx: 20                          Min Rx: 20          Multiplier: 3
Neg Tx: 4                           Neg Rx: 20          Neg detect mult: 3
Sess up time : 00:00:00
Sess down time : 00:00:00
Bind Application : VRRP
-----
```

Related Commands

None

13.13.11 show resource bfd static configurations

Command Purpose

Use this command to show the resource of static bfd configurations

Command Syntax

```
show resource bfd static configurations
```

Command Mode

User EXEC

Default

None

Usage

Use this command to show the resource of static BFD configurations

Examples

The following example is the result of this command:

```
Switch# show resource bfd static configurations
```

```
Switch# show resource bfd static configurations
```

```
BFD (Static-BFD, Vrrp-BFD)
```

```
Resource                Used                Capability
```

```
=====
```

```
BFD static configuration
```

Related Commands

13.13.12 show bfd interface

Command Purpose

Use this command to show the IP bfd interface statuses.

Command Syntax

```
show bfd interface ( IFNAME | all | )
```

Parameter	Parameter Description	Parameter Value
IFNAME	BFD Interface	Support physical/aggregation/vlan/ ports

Command Mode

Privileged EXEC

Default

N/A

Usage

Use this command to show the IP bfd interface statuses.

User can show the specified interface or all interfaces.

Examples

The following example is the result of this command:

```
Switch# show bfd interface eth-0-9
```

```
Interface:    eth-0-9  ifindex: 9 state:    UP
```

```
Interface level configuration: NO ECHO, NO SLOW TMR
```

```
Timers in Milliseconds
```

```
Min Tx: 1    Min Rx: 1    Multiplier: 3
```

Number of Sessions: 2

BFD discriminator: 8193 BFD state: DOWN

BFD discriminator: 8191 BFD state: DOWN

Related Commands

None

Chapter 14 Device Management Commands

14.1 STM Commands

14.1.1 stm prefer

Command Purpose

Use the `stm prefer` Global Configuration command to configure the profile used in Switch Table Management (STM) resource allocation. You can use profile to allocate system memory to best support the features being used in your application. Use profile to approximate the maximum number of unicast MAC addresses, quality of service (QoS) access control entries (ACEs) and unicast routes. Use the `no` form of this command to return to the default profile.

Command Syntax

`stm prefer ( default | layer2 | layer3 | ipv6 )`

`no stm prefer`

Parameter	Parameter Description	Parameter Value
default	Provide balance to all features	-
layer2	Provide maximum FDB entries. This profile maximizes system memory for use as a Layer 2 switch	-
layer3	Provide maximum Host Route/Indirect Route entries. You would typically use this profile for a router or aggregator in the middle of a network	-
ipv6	Unicast bias, supporting more IPv6 Ucast Routes. This profile is only existed when IPv6 feature is supported.	-

Command Mode

Global Configuration

Default

System use the default profile when first boot up, this profile balance all the features.

Usage

Users must reload the switch for the configuration to take effect.

Examples

This example shows how to configure the ipv4 profile on the switch: You can verify your settings by entering the show stm prefer in privileged EXEC mode:

```
Switch# configure terminal
Switch(config)# stm prefer layer3
Switch(config)# exit
Switch# reload
```

Related Commands

show stm prefer

14.1.2 show stm prefer

Command Purpose

Use the show stm prefer privileged EXEC command to display information about the profiles that can be used to maximize system resources for a particular feature, or use the command without a keyword to display the profile in use.

Command Syntax

show stm prefer (default | layer2 | layer3 | ipv6)
no stm prefer

Parameter	Parameter Description	Parameter Value
default	Provide balance to all features	-
layer2	Provide maximum FDB entries. This profile maximizes system memory for use as a Layer 2 switch	-
layer3	Provide maximum Host Route/Indirect Route entries. You would typically use this profile for a router or aggregator in the middle of a network	-
ipv6	Unicast bias, supporting more IPv6 Ucast Routes. This profile is only existed when IPv6 feature is supported.	-

Command Mode

Privileged EXEC

Default

None

Usage

If you did not reload the switch after entering the `stm prefer` Global Configuration command, the `show stm prefer` privileged EXEC command displays the profile currently in use and not the newly configured profile.

The numbers displayed for each profile represent an approximate maximum number for each feature resource.

Examples

This is an example of output from the `show stm prefer` command, displaying the profile currently in use:

```
Switch# show stm prefer
```

```
Current profile is :default
```

```

number of vlan instance           : 1/4094
number of unicast mac address     : 0/65536
number of multicast mac address   : 0/2048
number of blackhole mac address   : 0/128
number of max applied vlan mapping : 0/1024
number of bfd sessions            : 0/128
number of CFM loacl&remote MEPs   : 0/1024
number of CFM lm                  : 0/256
number of CFM lck                 : 0/24
number of G8031 groups            : 0/256
number of G8032 rings             : 0/256
number of G8032 member ports      : 0/256
number of mac based vlan class    : 0/512
number of ipv4 based vlan class    : 0/512
number of ipv6 based vlan class    : 0/0
number of dot1x mac based         : 0/2048
number of unicast ipv4 host routes : 0/4096
number of unicast ipv4 indirect routes : 0/8192
number of unicast ipv4 policy based routes : 0/16
number of unicast ipv6 host routes : 0/0
number of unicast ipv6 indirect routes : 0/0
number of unicast ecmp groups      : 0/240
number of unicast ip tunnel peers  : 0/8
number of multicast ipv4 routes    : 0/1023
number of mvr entries             : 0/511
number of mvr6 entries            : 0/0
number of multicast ipv6 routes    : 0/0
number of ipv4 source guard entries : 0/1024
number of ingress port acl flow entries : 0/2035
```

```
number of ingress vlan acl flow entries      : 0/255
number of egress port acl flow entries       : 0/255
number of ingress port qos flow entries      : 9/2043
number of ingress port acl ipv6 flow entries : 0/0
number of ingress vlan acl ipv6 flow entries : 0/0
number of egress port acl ipv6 flow entries  : 0/0
number of ingress port qos ipv6 flow entries : 0/0
number of link aggregation (static & lacp)   : 0/55
number of ipfix cache                        : 0/16384
```

Related Commands

stm prefer

14.2 Syslog Commands

14.2.1 clear logging buffer

Command Purpose

To clear messages from the logging buffer, use the clear logging buffer command in Privileged EXEC mode.

Command Syntax

```
clear logging buffer
```

Command Mode

Privileged EXEC

Default

None

Usage

Clear log messages in logging buffer

Examples

The following shows how to clear logging buffer:

```
Switch# clear logging buffer
```

Related Commands

show logging buffer

14.2.2 logging alarm-trap

Command Purpose

To limit messages logged to the syslog servers based on severity, use the logging alarm-trap command in Global Configuration mode. To restore the default level, use the no form of this command.

Command Syntax

logging alarm-trap (enable | disable | level (high | lower | middle | minor))

no logging alarm-trap level

Parameter	Parameter Description	Parameter Value
enable	Enable logging traps	-
disable	Disable logging traps	-
level high	The high alarm level	-
level lower	The lower alarm level.	-
level middle	The middle alarm level	-
level minor	The minor alarm level	-

Command Mode

Global Configuration

Default

Logging trap is disabled.

Usage

A trap is an unsolicited message sent to a remote network management host. Logging traps should not be confused with SNMP traps.

Examples

The following shows how to limit messages logged to the log servers based on severity:

```
Switch# configure terminal
Switch(config)# logging alarm-trap enable
Switch(config)# logging alarm-trap level high
```

Related Commands

logging alarm-trap level middle

14.2.3 logging file

Command Purpose

To enable writing logs into files, use the logging file command in Global Configuration mode.

Command Syntax

logging file (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Enable writing logs to file	-
disable	Disable writing logs to file	-

Command Mode

Global Configuration

Default

Logging file is enabled

Usage

If logging file will enabled, the log will be saved to flash:/syslog every 6 hours.

Examples

The following shows how to enable logging file function:

```
Switch# configure terminal
Switch(config)# logging file enable
```

Related Commands

show logging

14.2.4 logging level file

Command Purpose

To set severity level while writing logs into files, use the logging level file command in Global Configuration mode. To return the logging to the default level, use the no form of this command.

Command Syntax

logging level file (alert | critical | debug | emergency | error | information | notice | warning | *SEVERITY_LEVEL*)

no logging level file

Parameter	Parameter Description	Parameter Value
0 emergency	System is unusable	-
1 alert	Immediate action needed	-
2 critical	Critical conditions	-
3 error	Error conditions	-
4 warning	Warning conditions	-
5 notice	Normal but significant conditions	-
6 information	Informational messages	-
7 debug	Debugging messages	-
SEVERITY_LEVEL	Severity level	0-7

Command Mode

Global Configuration

Default

Logging file level is information.

Usage

Specifying a severity-level causes messages only at that level and numerically lower levels to files.

Examples

In the following example, the user specifies that only messages of the levels error, critical, alerts, and emergency be logged to files:

```
Switch# configure terminal
Switch(config)# logging level file 3
```

Related Commands

logging level module

14.2.5 logging buffer

Command Purpose

To set the number of logs saved in system buffer, use the logging buffer command in Global Configuration mode. To return the logging to the default value, use the no form of this command.

Command Syntax

logging buffer *BUFFERSIZE*

no logging buffer

Parameter	Parameter Description	Parameter Value
BUFFERSIZE	logging buffer size	10-1000

Command Mode

Global Configuration

Default

500

Usage

Specifying the max number of messages showed in CLI show logging buffer.

Examples

In the following example, the user save 1000 logging entries in system:

```
Switch# configure terminal
```

```
Switch(config)# logging buffer 1000
```

Related Commands

show logging buffer

14.2.6 logging level module

Command Purpose

To set severity level, use the logging level module command in Global Configuration mode. To return the logging to the default level, use the no form of this command.

Command Syntax

logging level module (alert | critical | debug | emergency | error | information | notice | warning | *SEVERITY_LEVEL*)

no logging level module

Parameter	Parameter Description	Parameter Value
0 emergency	System is unusable	-
1 alert	Immediate action needed	-
2 critical	Critical conditions	-
3 error	Error conditions	-
4 warning	Warning conditions	-
5 notice	Normal but significant conditions	-
6 information	Informational messages	-
7 debug	Debugging messages	-
SEVERITY_LEVEL	Severity level	0-7

Command Mode

Global Configuration

Default

Logging file level is debugging.

Usage

Specifying a severity-level causes messages only at that level and numerically lower levels of the modules.

Examples

In the following example, the user specifies that all messages be logged:

```
Switch# configure terminal
Switch(config)# logging level module debug
```

Related Commands

logging level file

14.2.7 logging merge

Command Purpose

To enable the logging merge, use the logging merge command in Global Configuration mode. To restore to default value, use the no form of this command.

Command Syntax

logging merge (enable | disable | fifo-size *SIZE* | timeout *SECONDS*)

no logging merge (fifo-size | timeout)

Parameter	Parameter Description	Parameter Value
enable	Enable logging mergence	-
disable	Disable logging mergence	-
fifo-size <i>SIZE</i>	Set fifo size. The range is 100 to 10240, default value is 1024	100-10240
timeout <i>SECONDS</i>	Set timeout. The range is 1 to 300 seconds, default value is 10 seconds	1-300

Command Mode

Global Configuration

Default

Logging mergence is enabled.

Usage

The logging merge command merges all the same logs into one during a specified time range. During this time, the switch buffered these same logs. You can use the timeout keyword to set the time range, and use the fifo-size to set the buffer size.

Examples

The following shows how to enable logging merge function:

```
Switch# configure terminal
Switch(config)# logging merge enable
```

Related Commands

logging merge timeout 30

14.2.8 logging sync

Command Purpose

To synchronize log from buffer to syslog file, use the logging sync command in privileged EXEC mode.

Command Syntax

logging sync

Command Mode

Privileged EXEC

Default

None

Usage

When enabled log merge, system will merge all the same logs into one during a specified time range. During this time log will not send to logging buffer. If user wants to sync log to logging buffer, use this command. And synchronize log from buffer to syslog file.

Examples

The following shows how to enable logging sync function:

```
Switch# logging sync
```

Related Commands

logging merge enable logging sync timeout

14.2.9 logging sync timeout**Command Purpose**

To set the timeout that synchronize log from buffer to syslog file. To restore to default value, use the no form of this command.

Command Syntax

logging sync timeout *INTERVAL*

no logging sync timeout

Parameter	Parameter Description	Parameter Value
INTERVAL	sync timeout in minutes	5-1440

Command Mode

Global Configuration

Default

360 minutes

Usage

None

Examples

The following shows how to set every 5 minutes synchronize log from buffer to syslog file:

```
Switch# configure terminal
Switch(config)# logging sync timeout 5
```

Related Commands

logging sync

14.2.10 logging operate

Command Purpose

To log the operations, and use the logging operate command in Global Configuration mode.

Command Syntax

logging operate (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Enable logging operations	-
disable	Disable logging operations	-

Command Mode

Global Configuration

Default

Logging operations is disabled

Usage

If logging operate is enabled, all the CLI in configure mode or higher will be save to logger buffer.

Examples

The following shows how to enable logging operate function:

```
Switch# configure terminal
Switch(config)# logging operate enable
```

Related Commands

logging server

14.2.11 logging server

Command Purpose

To enable the logging to the remote logging servers, use the logging server command in Global Configuration mode.

Command Syntax

logging server (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Enable logging server	-
disable	Disable logging server	-

Command Mode

Global Configuration

Default

Logging operations is disabled.

Usage

This command is used to send logger to a remote server.

Examples

The following shows how to use logging server command:

```
Switch# configure terminal
Switch(config)# logging server enable
```

Related Commands

logging server severity

14.2.12 logging server address

Command Purpose

To log system messages and debug output to a remote server, use the logging server address command in Global Configuration mode. To remove a specified logging server from the configuration, use the no form of this command.

Command Syntax

logging server address (mgmt-if |) (IPV4_ADDR | IPV6_ADDR) (source-interface IFNAME | source-ip SRC_IP_ADDR |)

no logging server address (mgmt-if |) (IPV4_ADDR | IPV6_ADDR)

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
IPV4_ADDR	IPv4 address of the server that will receive the system logging messages	IPv4 Address
IPV6_ADDR	IPv6 address of the server that will receive the system logging messages	IPv6 Address
IFNAME	Name of source interface	All interface type
SRC_IP_ADDR	Source IP address	IPv4 Address

Command Mode

Global Configuration

Default

System logging messages are not sent to any remote server.

Usage

The logging server address command identifies a remote server (usually a device serving as a syslog server) to receive logging messages. By issuing this command more than once, you can build a list of servers that receive logging messages.

If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

In the following example, messages are logged to a server at 209.165.202.169:

```
Switch# configure terminal
```

```
Switch(config)# logging server address 209.165.202.169
```

Related Commands

logging server

14.2.13 logging server facility

Command Purpose

To configure the syslog facility in which error messages are sent, use the logging server facility command in Global Configuration mode. To revert to the default of local7, use the no form of this command.

Command Syntax

logging server facility (kern | user | mail | daemon | auth | syslog | lpr | news | uucp | cron | authpriv | ftp | *FACILITY_TYPE* | *FACILITY_LOCAL*)

no logging server facility

Parameter	Parameter Description	Parameter Value
0 kern	Kernel	-
1 user	User	-
2 mail	Mail system	-
3 daemon	System daemon	-
4 auth	Authorization system	-
5 syslog	System log	-
6 lpr	Line printer system	-
7 news	USENET news	-
8 uucp	UNIX-to-UNIX	-
9 cron	Cron facility	-
10 authpriv	Authorization priv system	-
11 ftp	FTP system	-
16 local0	Reserved for locally defined messages	-
17 local1	Reserved for locally defined messages	-
18 local2	Reserved for locally defined messages	-
19 local3	Reserved for locally defined messages	-
20 local4	Reserved for locally defined messages	-
21 local5	Reserved for locally defined messages	-
22 local6	Reserved for locally defined messages	-

Parameter	Parameter Description	Parameter Value
23 local7	Reserved for locally defined messages	-
FACILITY_TYPE	system defined messages	0-11
FACILITY_LOCAL	Reserved for locally defined messages	6-23

Command Mode

Global Configuration

Default

Default is local4

Usage

None

Examples

The following shows how to use logging file command:

```
Switch# configure terminal
Switch(config)# logging server facility local3
```

Related Commands

logging server

14.2.14 logging server severity

Command Purpose

To set severity level while writing logs into servers, use the logging server severity command in Global Configuration mode. To revert to the default severity level, use the no form of this command.

Command Syntax

```
logging server severity ( alert | critical | debug | emergency | error | information | notice | warning | SEVERITY_LEVEL )
no logging server severity
```

Parameter	Parameter Description	Parameter Value
0 emergency	System is unusable	-
1 alert	Immediate action needed	-
2 critical	Critical conditions	-
3 error	Error conditions	-
4 warning	Warning conditions	-
5 notice	Normal but significant conditions	-
6 information	Informational messages	-
7 debug	Debugging messages	-
SEVERITY_LEVEL	Severity level	0-7

Command Mode

Global Configuration

Default

Logging server level is information.

Usage

This command is used to set severity level while writing logs into servers.

Examples

In the following example, the user specifies that only messages of the levels error, critical, alerts, and emergency be logged to server:

```
Switch# configure terminal
Switch(config)# logging server severity 3
```

Related Commands

logging level module

logging level file

14.2.15 logging timestamp

Command Purpose

To configure the system to apply a time-stamp to debugging messages or system logging messages, use the logging timestamps command in Global Configuration mode. To restore the default timestamp format, use the no form of this command.

Command Syntax

logging timestamp (`bsd` | `date` | `iso` | `none` | `rfc3164` | `rfc3339`)

no logging timestamp

Parameter	Parameter Description	Parameter Value
bsd	BSD style (RFC 3164)	-
date	Date command style	-
iso	ISO style (RFC 3339)	-
none	No timestamp	-
rfc3164	RFC 3164 style (bsd)	-
rfc3339	RFC 3339 style (iso)	-

Command Mode

Global Configuration

Default

Default timestamp format is BSD.

Usage

This command is used to specify the timestamp in logger message.

Examples

The following shows how to set the timestamp to iso.:

```
Switch# configure terminal
```

```
Switch(config)# logging timestamp iso
```

Related Commands

`show logging`

14.2.16 show logging

Command Purpose

To display the state of system logging (syslog), use the `show logging` command in privileged EXEC mode.

Command Syntax

show logging

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following shows how to display the configuration of the log:

```
Switch# show logging
```

```
Current logging configuration:
```

```
=====
logging buffer 500
logging timestamp date
logging file enable
logging level file warning
logging level module debug
logging server disable
logging server severity warning
logging server facility local7
logging alarm-trap enable
logging alarm-trap level middle
logging merge disable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

Related Commands

logging level

14.2.17 show logging buffer

Command Purpose

To display the contents of the standard system logging buffer, use the show logging buffer command in privileged EXEC mode.

Command Syntax

show logging buffer (*LINES* | statistics |)

Parameter	Parameter Description	Parameter Value
LINES	Specify the max number of logs.positive number means latest message displayed on top, negative number means the oldest message displayed on top.	-1000-1000
statistics	Display statistics of logging buffers	-

Command Mode

Privileged EXEC

Default

Display 20 messages when messages number is not specified. The latest message is displayed on top

Usage

None

Examples

The following shows how to use show logging buffer command:

```
Switch# show logging buffer statistics
```

```
Logging buffer statistics:
```

```
=====
```

```
Total processed 153 entries
```

```
Total dropped 0 entries
```

```
Current have 153 entries
```

```
The latest message is:
```

```
Aug  6 16:06:44 Switch3 IMISH-6: ready to service
```

```
The oldest message is:
```

```
Aug  6 13:38:38 Switch LOGGING-5: logging starting up; version='\2.0rc4\'
```

Related Commands

show logging

14.3 Mirror Commands

14.3.1 monitor session destination interface

Command Purpose

Use this command to set mirror destination interface.

To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* destination interface *IFNAME*

no monitor session *SESSION* destination

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
IFNAME	mirror destination interface	Support aggregation, physical and tunnel interfaces

Command Mode

Global Configuration

Default

None

Usage

Same session can't configure both local destination interface and remote destination VLAN.(About the remote destination VLAN, please refer to chapter "monitor session destination remote".)

Examples

This example shows how to set the mirror destination port to eth-0-1 in session 1:

```
Switch# configure terminal
```

```
Switch(config)# monitor session 1 destination interface eth-0-1
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)# no monitor session 1 destination
```

Related Commands

monitor session *SESSION-ID* source interface

monitor session SESSION-ID source vlan
show monitor

14.3.2 monitor session destination cpu

Command Purpose

Use this command to set mirror destination of cpu.
To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* destination cpu
no monitor session *SESSION-ID* destination

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
destination cpu	mirror destination cpu	-

Command Mode

Global Configuration

Default

None

Usage

The destination can be cpu port.
Same session can't configure both destination cpu and remote destination VLAN.(About the remote destination VLAN, please refer to chapter "monitor session destination remote".)

Examples

This example shows how to set the mirror destination to cpu in session 1:

```
Switch# configure terminal  
Switch(config)# monitor session 1 destination cpu
```

This example shows how to remove this setting:

```
Switch# configure terminal  
Switch(config)# no monitor session 1 destination
```

Related Commands

monitor session SESSION-ID source interface
monitor session SESSION-ID source vlan
show monitor

14.3.3 monitor session destination group

Command Purpose

Use this command to create mirror multi destination group and enter mirror destination group mode.
To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* destination group *GROUP-ID*
no monitor session *SESSION-ID* destination

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
Destination group GROUP-ID	mirror destination group id number	1-32

Command Mode

Global Configuration

Default

None

Usage

Only one session can configure to multi-dest group. The session type only support local destination interface. One session can have multi destination group members which port is physical port. Same session can't configure both local destination interface and remote destination VLAN.(About the remote destination VLAN, please refer to chapter "monitor session destination remote".)

Examples

This example shows how to create the mirror to multi-destination group in session 1.:

```
Switch# configure terminal
```

```
Switch(config)# monitor session 1 destination group 1
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)# no monitor session 1 destination
```

Related Commands

monitor session SESSION-ID source interface
member
show monitor

14.3.4 member

Command Purpose

Use this command to add a group member mirror destination interface for a mirror destination group.
To remove this setting, use the no form of this command.

Command Syntax

member *IFPHYSICAL*

Parameter	Parameter Description	Parameter Value
IFPHYSICAL	mirror destination interface	Support physical ports

Command Mode

Mirror Destination Group Configuration

Default

None

Usage

The destination interface only can be physical port. It can be neither VLAN interface nor Aggregator interface.
Same session can't configure both local destination interface and multi-destination interface

Examples

This example shows how to add the mirror destination eth-0-1 to group of multi-destination session:

```
Switch# configure terminal
Switch(config)# monitor session 1 destination group 1
Switch(config-monitor-d-group)# member eth-0-1
```

This example shows how to remove this setting:

```
Switch# configure terminal
Switch(config)# monitor session 1 destination group 1
Switch(config-monitor-d-group)# no member eth-0-1
```

Related Commands

monitor session SESSION-ID source interface
monitor session SESSION-ID destination group GROUP-ID
show monitor

14.3.5 monitor session source interface

Command Purpose

Command Syntax

monitor session *SESSION-ID* source interface interface (both | tx | rx)
no monitor session *SESSION-ID* source interface *IFNAME* (both | tx | rx)

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
Parameter	Parameter Description	Parameter Value
source interface IFNAME	mirror source interface	Support aggregation and physical interfaces
both	monitor received and transmitted traffic on that interface	-
rx	monitor received traffic only on that interface	-
tx	monitor transmitted traffic only on that interface	-

Command Mode

Global Configuration

Default

None

Usage

The mirror source interface can be either physical port or Aggregator interface. (e.g. eth-0-1, agg1).
If the parameter for direction [both|tx|rx] is not specified, the default value is both.

Examples

This example shows how to remove this setting.:

```
Switch# configure terminal
```

```
Switch(config)# no monitor session 1 source interface eth-0-11
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)# no monitor session 1 source interface eth-0-11
```

Related Commands

monitor session *SESSION-ID* destination

show monitor

14.3.6 monitor session source vlan

Command Purpose

Use this command to set mirror source vlan.

To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* source vlan *VLAN-ID* (both | tx | rx)

no monitor session *SESSION-ID* source vlan *VLAN-ID* (both | tx | rx)

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
VLAN-ID	the source vlan id to be mirrored	1-4094
both	monitor received and transmitted traffic on that interface	-
rx	monitor received traffic only on that interface	-
tx	monitor transmitted traffic only on that interface	-

Command Mode

Global Configuration

Default

None

Usage

If the parameter for direction (both|tx|rx) is not specified, the default value is both.

Before configure the monitor session source vlan, User should create vlan by command "vlan database", and create vlan interface by command "interface vlan" first.

Examples

This example shows how to create vlan and vlan interface:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface vlan2
Switch(config-if)# exit
```

This example shows how to set the mirror source to vlan2 in session 1:

```
Switch# configure terminal
Switch(config)# monitor session 1 source vlan 2 both
```

This example shows how to set the mirror source to vlan2 in session 1 to monitor received traffic only:

```
Switch# configure terminal
Switch(config)# monitor session 1 source vlan 2 rx
```

This example shows how to set the mirror source to vlan2 in session 1 to monitor transmitted traffic only:

```
Switch# configure terminal
Switch(config)# monitor session 1 source vlan 2 tx
```

This example shows how to remove this setting:

```
Switch# configure terminal
Switch(config)# no monitor session 1 source vlan 2 both
```

This example shows how to delete vlan and vlan interface:

```
Switch# configure terminal
Switch(config)# no interface vlan2
Switch(config)# vlan database
Switch(config-vlan)# no vlan 2
Switch(config-vlan)# exit
```

Related Commands

monitor session destination
show monitor
vlan database
vlan VLAN-ID
interface vlan VLAN-ID

14.3.7 monitor session source cpu

Command Purpose

Use this command to set mirror source cpu

To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* source cpu (both | tx | rx)

no monitor session *SESSION-ID* source cpu (both | tx | rx)

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
cpu	set cpu to be mirrored	-
both	monitor received and transmitted traffic on that interface	-
rx	monitor received traffic only on that interface	-
tx	monitor transmitted traffic only on that interface	-

Command Mode

Global Configuration

Default

None

Usage

If the parameter for direction (both|tx|rx) is not specified, the default value is both.

Mirror source cpu can only be configured in session 1.

Examples

This example shows how to set the mirror source to cpu in session 1:

```
Switch# configure terminal
```

```
Switch(config)# monitor session 1 source cpu both
```

This example shows how to set the mirror source to cpu in session 1 to monitor received traffic only:

```
Switch# configure terminal
```

```
Switch(config)# monitor session 1 source cpu rx
```

This example shows how to set the mirror source to cpu in session 1 to monitor transmitted traffic only:

```
Switch# configure terminal
```

```
Switch(config)# monitor session 1 source cpu tx
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)#no monitor session 1 source cpu both
```

Related Commands

monitor session destination

show monitor

14.3.8 monitor session destination interface tunnel

Command Purpose

Use this command to set erspan mirror destination interface tunnel.

To remove this setting, use the no form of this command.

Command Syntax

monitor session SESSION-ID destination interface IFTUNNEL

no monitor session SESSION-ID destination interface IFTUNNEL

Parameter	Parameter Description	Parameter Value
SESSION-ID	<1-3> mirror session number	1-3
IFTUNNEL	<0-1023> ERSPAN monitor destination tunnel	0-1023

Command Mode

Global Configuration

Default

None

Usage

The destination tunnel and its mode should be created before configuring ERSPAN monitor destination.

The ERSPAN destination interface can only be a tunnel interface.

About tunnel configuration, please refer to "IPv6_Service_CLI_en.doc"

Examples

This example shows how to create the tunnel::

```
Switch# configure terminal
Switch (config)# interface tunnel
Switch (config-vlan)# tunnel mode erspan
Switch (config-vlan)# exit
```

This example shows how to set the ERSPAN mirror destination to tunnel1 in session 1::

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface tunnel1
```

This example shows how to remove this setting::

```
Switch# configure terminal
Switch(config)# no monitor session 1 destination
```

This example shows how to delete the tunnel::

```
Switch# configure terminal
Switch (config)# no interface tunnel1
Switch (config-vlan)# exit
```

Related Commands

monitor session SESSION-ID source interface

monitor session SESSION-ID source vlan

interface tunnel

tunnel mode mode

14.3.9 monitor session destination remote

Command Purpose

Use this command to set mirror remote destination vlan and interface.

To remove this setting, use the no form of this command.

Command Syntax

monitor session *SESSION-ID* destination remote vlan *VLAN-ID* interface *IFNAME*

no monitor session *SESSION-ID* destination remote vlan

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3
VLAN-ID	Remote mirror destination VLAN id	2-4094
IFNAME	the out-going interface for mirrored packets	Support physical interface

Command Mode

Global Configuration

Default

None

Usage

The destination vlan should be created in vlan database.

The destination interface can only be physical port.

To prevent another copy of packets flood out from the destination outgoing port, user can remove the port from default vlan by command "switchport trunk allowed vlan remove 1".

Examples

This example shows how to create the vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# exit
```

This example shows how to set the mirror remote destination vlan to 2 and outgoing port to eth-0-1 in session 1:

```
Switch# configure terminal
Switch(config)# monitor session 1 destination remote vlan 2 interface eth-0-1
```

This example shows how to remove this setting:

```
Switch# configure terminal
Switch(config)# no monitor session 1 destination remote vlan
```

This example shows how to delete the vlan:

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# no vlan 2
Switch(config-vlan)# exit
```

Related Commands

monitor session SESSION-ID source interface

monitor session SESSION-ID source vlan

vlan database

vlan VLAN-ID

14.3.10 monitor mac escape

Command Purpose

Use this command to set remote mirror Mac escape feature. When these escape entries are set, the packets with specified MAC-DA will not be mirrored to the remote destination vlan when using Rspan(unsupported ERSPAN) .

To remove this setting, use the no form of this command.

Command Syntax

monitor mac escape *MAC MASK*

no monitor mac escape (*MAC MASK* |)

Parameter	Parameter Description	Parameter Value
MAC	mac address	mac address in HHHH. HHHH. HHHH format
MASK	mac address mask	mac address mask in HHHH. HHHH. HHHH format

Command Mode

Global Configuration

Default

None

Usage

Mac escape is used for remote mirror. It will not affect the result of local mirror.

If a Mac escape entry is set, the packet with this Mac destination can not be mirrored in remote mirror.

Command "no monitor mac escape " should delete the specified entry.

Command "no monitor mac escape" should delete all entries.

Examples

This example shows how to set the mirror mac escape:

```
Switch# configure terminal
```

```
Switch(config)# monitor mac escape 00cc.1122.3344 ffff.ffff.0000
```

This example shows how to remove this setting:

```
Switch# configure terminal
```

```
Switch(config)# no monitor mac escape 00cc.1122.3344 ffff.ffff.0000
```

Related Commands

monitor session *SESSION-ID* destination remote

14.3.11 show monitor

Command Purpose

Use this command to show the information about monitor.

Command Syntax

show monitor (session *SESSION-ID*)

Parameter	Parameter Description	Parameter Value
SESSION-ID	mirror session number	1-3

Command Mode

Privileged EXEC

Default

None

Usage

If session id is not specified, any configured sessions should be shown.

Examples

This example shows how to display the information about monitor:

```
DUT1# show monitor
```

```
session 1
```

```
Session    1
```

```
-----
```

```
Status      : Valid
```

```
Type        : Local Session
```

```
Source Ports :
```

```
  Receive Only :
```

```
  Transmit Only :
```

```
  Both         : eth-0-2
```

```
Source VLANs :
```

```
  Receive Only :
```

```
  Transmit Only :
```

```
  Both         :
```

```
Destination Port : eth-0-1
```

Related Commands

monitor session *SESSION-ID* source interface

monitor session SESSION-ID source vlan
monitor session SESSION-ID source cpu
monitor session SESSION-ID destination interface
monitor session SESSION-ID destination remote
monitor session SESSION-ID destination cpu

14.3.12 show monitor mac escape

Command Purpose

Use this command to show mac escape settings for remote mirror.

Command Syntax

show monitor mac escape

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the information about monitor mac escape:

```
Switch# show monitor mac escape

-----
monitor rspan mac escape database
-----
count    : 1
-----
Mac      : 00:cc:11:22:33:44
Mask     : ff:ff:ff:ff:00:00
-----
```

Related Commands

monitor mac escape MAC MASK

14.3.13 monitor destination forwarding enable

Command Purpose

Use this command to set mirror destination port forwarding enable.

To remove this setting, use the no form of this command.

Command Syntax

monitor destination forwarding enable

no monitor destination forwarding enable

Command Mode

Global Configuration

Default

Disabled

Usage

If any mirror destination is configured, this feature can't be changed.

Examples

This example shows how to set mirror destination forwarding enable:

```
Switch# configure terminal
```

```
Switch(config)# monitor destination forwarding enable
```

Related Commands

monitor session SESSION-ID destination

show monitor

14.3.14 monitor cpu set packet buffer

Command Purpose

Use this command to set mirror cpu buffer size, its default value is 1000 of packets.

To remove this setting, use the no form of this command.

Command Syntax

monitor cpu set packet buffer *SIZE*

no monitor cpu set packet buffer

Parameter	Parameter Description	Parameter Value
SIZE	buffer size in packets	1-1000, unit:packet

Command Mode

Global Configuration

Default

Default 1000

Usage

The mirror cpu buffer can store up to 1000 packets and the default value is 1000.

Examples

This example shows how to set mirror cpu buffer size:

```
Switch# configure terminal
```

```
Switch(config)# monitor cpu set packet buffer 50
```

Related Commands

show monitor cpu packet buffer size

14.3.15 monitor cpu capture packet

Command Purpose

Use this command to capture packets to be written in a text file from cpu memory buffer.

Command Syntax

monitor cpu capture packet (start | stop)

Parameter	Parameter Description	Parameter Value
start	start capture	-
stop	stop capture	-

Command Mode

Privileged EXEC

Default

Stop

Usage

When start capturing packet, the cpu mirror packets will be written in a text file and the file name is assigned by system. The text file is stored in the directory of flash/mirror/

Examples

This example shows how to start cpu capturing packets in a text file:

```
Switch# configure terminal
```

```
Switch(config)# monitor cpu capture packet start
```

This example shows how to stop cpu capturing packets in a text file:

```
Switch# configure terminal
```

```
Switch(config)# monitor cpu capture packet stop
```

Related Commands

pcap convert FILENAMEA FILENAMEB

14.3.16 monitor cpu capture strategy

Command Purpose

Use this command to set the strategy of capturing packets.

Command Syntax

monitor cpu capture strategy (replace | drop)

Parameter	Parameter Description	Parameter Value
replace	the oldest packet would be replaced by the latest packet when cpu mirror memory buffer is full	-
drop	the latest packet would be discard when cpu mirror memory buffer is full	-

Command Mode

Global Configuration

Default

Replace

Usage

None

Examples

This example shows how to set cpu capture strategy as replace:

```
Switch# configure terminal
```

```
Switch(config)# monitor cpu capture strategy replace
```

This example shows how to set cpu capture strategy as drop:

```
Switch# configure terminal
```

```
Switch(config)# monitor cpu capture strategy drop
```

Related Commands

show monitor cpu capture strategy

14.3.17 show monitor cpu packet

Command Purpose

Use this command to show the mirror cpu packets in memory.

Command Syntax

show monitor cpu packet (all | *PACKET-ID*)

Parameter	Parameter Description	Parameter Value
all	show all of mirror cpu packets in memory	-
PACKET-ID	show the mirror cpu packets of user specifying	1-1000

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the all mirror cpu packets in memory:

```
Switch(config)# show monitor cpu packet all
```

Related Commands

monitor session SESSION-ID destination cpu

14.3.18 clear monitor cpu packet all

Command Purpose

Use this command to clear the mirror cpu packets in memory.

Command Syntax

clear monitor cpu packet all

Command Mode

Privileged EXEC

Default

None

Usage

clear all the mirror cpu packets in memory.

Examples

This example shows how to clear all the mirror cpu packets in memory buffer:

```
Switch(config)# clear monitor cpu packet all
```

Related Commands

show monitor cpu packet (all|<1-1000>)

14.3.19 show monitor cpu packet buffer-size

Command Purpose

Use this command to show the buffer size of mirror cpu in memory

Command Syntax

show monitor cpu packet buffer-size

Command Mode

Privileged EXEC

Default

None

Usage

It displays the mirror cpu buffer size in memory and the size intends the number of packets.

Examples

This example shows how to show the mirror cpu buffer size in memory:

```
Switch(config)# show monitor cpu packet buffer-size
```

Related Commands

monitor cpu set packet buffer <1-1000>

14.3.20 show monitor cpu capture strategy

Command Purpose

Use this command to show the current strategy of capturing packets.

Command Syntax

show monitor cpu capture strategy

Command Mode

Privileged EXEC

Default

None

Usage

It display the current strategy of capturing mirror cpu packets in memory.

Examples

This example shows how to show the current capture strategy:

```
Switch(config)# show monitor cpu capture strategy
```

Related Commands

monitor cpu capture strategy (replace|drop)

14.4 Device Management Commands

14.4.1 Temperature

Command Purpose

To specify the system temperature monitor threshold.

Command Syntax

temperature *LOW HIGH CRITICAL*

no temperature

Parameter	Parameter Description	Parameter Value
LOW	Low alarm temperature degree Celsius	45-50, unit:degree Celsius
HIGH	High alarm temperature degree Celsius	50-85, unit:degree Celsius

Parameter	Parameter Description	Parameter Value
CRITICAL	Critical alarm temperature degree Celsius	55-100, unit:degree Celsius

Command Mode

Global Configuration

Default

The default threshold is low temperature 5, high temperature 75, and critical temperature 90.

Usage

The unit for temperature is centigrade.

The critical temperature must higher than high temperature 5 Celsius degrees.

The high temperature must higher than low temperature 5 Celsius degrees.

Examples

This example shows how to specify the temperature thresholds:

```
Switch# configure terminal
Switch(config)# temperature 5 70 90
```

Related Commands

show environment

14.4.2 show environment

Command Purpose

Use this command to show the hardware environment information.

Command Syntax

show environment (slot *ID* |)

Parameter	Parameter Description	Parameter Value
ID	The ID of stack member.	1-29

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display hardware environment information:

```
Switch# show environment
```

Fan tray status:

Index	Status
1	PRESENT

FanIndex	Status	SpeedRate	Mode
1-1	OK	30%	Auto
1-2	OK	30%	Auto
1-3	OK	30%	Auto

Power status:

Index	Status	Power	Type	Alert
1	PRESENT	OK	AC	NO
2	ABSENT	-	-	-

Sensor status (Degree Centigrade):

Index	Temperature	Lower_alarm	Upper_alarm	Critical_limit
1	64	5	75	90

Related Commands

Temperature

14.4.3 boot system

Command Purpose

Use this command to specify the system image that the switch loads at startup.

Command Syntax

```
boot system ( GFLASHFILE | tftp: mgmt-if IP_ADDR GTFTPFLIE )
```

Parameter	Parameter Description	Parameter Value
GFLASHFILE	The file name that will be used to load at startup	File path and name on the flash
IP_ADDR	The tftp server IP address	IPv4 Address
tftp: mgmt-if	Use management port	-
GTFTPFLIE	The file name that will be used to load at startup	File name on the tftp server

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to specify load image from tftp when switch startup:

```
Switch# boot system tftp: mgmt-if 10.10.29.160 ulmage.r
```

Related Commands

None

14.4.4 show transceiver

Command Purpose

Use this command to show the transceiver information.

Command Syntax

```
show transceiver ( interface | ) ( detail | )
```

Parameter	Parameter Description	Parameter Value
interface	Specify the physical interface	-
detail	Show detail include DDM information	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display transceiver information:

```
Switch# show transceiver detail
```

```
Port eth-1-2 transceiver info:
```

```
Transceiver Type: 10G Base-SR
```

```
Transceiver Vendor Name : OEM
```

```
Transceiver PN           : SFP-10GB-SR
```

```
Transceiver S/N          : 201033PST1077C
```

```
Transceiver Output Wavelength: 850 nm
```

```
Supported Link Type and Length:
```

```
    Link Length for 50/125um multi-mode fiber: 80 m
```

```
    Link Length for 62.5/125um multi-mode fiber: 30 m
```

```
-----
```

Transceiver is internally calibrated.

mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.

++ : high alarm, + : high warning, - : low warning, -- : low alarm.

The threshold values are calibrated.

		High Alarm	High Warn	Low Warn	Low Alarm
Temperature	Threshold	Threshold	Threshold	Threshold	Threshold
Port (Celsius)	(Celsius)	(Celsius)	(Celsius)	(Celsius)	(Celsius)
eth-1-2	25.92	95.00	90.00	-20.00	-25.00

		High Alarm	High Warn	Low Warn	Low Alarm
Voltage	Threshold	Threshold	Threshold	Threshold	Threshold
Port (Volts)	(Volts)	(Volts)	(Volts)	(Volts)	(Volts)
eth-1-2	3.32	3.80	3.70	2.90	2.80

	Current	High Alarm	High Warn	Low Warn	Low Alarm
Port	(milliamperes)	Threshold (mA)	Threshold (mA)	Threshold (mA)	Threshold (mA)
eth-1-2	6.41	20.00	18.00	1.00	0.50

	Optical	High Alarm	High Warn	Low Warn	Low Alarm
Port	Transmit Power (dBm)	Threshold (dBm)	Threshold (dBm)	Threshold (dBm)	Threshold (dBm)
eth-1-2	-2.41	2.01	1.00	-6.99	-7.96

	Optical	High Alarm	High Warn	Low Warn	Low Alarm
Port	Receive Power (dBm)	Threshold (dBm)	Threshold (dBm)	Threshold (dBm)	Threshold (dBm)
eth-1-2	-12	- 1.00	0.00	-19.00	-20.00

Related Commands

None

14.4.5 update bootrom

Command Purpose

Use this command to update bootrom image.

Command Syntax

update bootrom (flash | udisk)

Parameter	Parameter Description	Parameter Value
flash	Source file direction	-
udisk	Source file direction	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to update bootrom image:

```
Switch# configure terminal
Switch(config)# update bootrom flash:/boot/ bootrom.bin
```

Related Commands

None

14.4.6 show reboot-info**Command Purpose**

Use this command to show reboot info.

Command Syntax

show reboot-info (slot *ID* |)

Parameter	Parameter Description	Parameter Value
ID	The ID of stack member.	1-29

Command Mode

Privileged EXEC

Default

None

Usage

Reboot Type	Description
POWER	Power outages
MANUAL	Cli "reboot/reload" undersystem
HIGH-TMPR	Reboot for abnormal high temperature
BHMDOG	BHM watchdog, monitor functional module
LCMDOG	LCM watchdog, monitor each LC
SCHEDULE	Schedule reboot

Reboot Type	Description
SNMP-RELOAD	SNMP reboot
HALFAIL	Reboot for HAGT communicate with HSRV failed, need stack enable
ABNORMAL	Unusual reboot, include reboot under shell
CTCINTR	Button reboot
LCATTACH	Reboot for LC attach CHSM failed
OTHER	Other reboot
OTHER	Other reboot

Examples

This example shows how to show reboot-info:

Switch# show reboot-info

Times	Reboot Type	Reboot Time
1	MANUAL	2016/09/08 15:14:41
2	MANUAL	2016/09/08 14:23:31
3	MANUAL	2000/01/01 00:00:01
4	HIGH-TMPR	2000/01/01 01:01:40
5	MANUAL	2000/01/01 00:08:17
6	ABNORMAL	1959/11/25 17:44:24
7	MANUAL	1959/11/26 14:51:37
8	MANUAL	1959/11/28 09:04:35
9	MANUAL	2016/09/12 09:44:53
10	MANUAL	2000/01/01 00:00:01

Related Commands

None

14.5 Bootrom Commands

14.5.1 Version

Command Purpose

Use the version command to show the Bootrom version information.

Command Syntax

Version

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to show the U-boot version:

```
bootrom:> version
```

```
U-Boot 2013.01-svn11932 (Sep 01 2015 - 17:12:25) - V8.1.0
powerpc-fsl_networking-linux-gnuspe-gcc (GCC) 4.7.2
GNU ld (GNU Binutils) 2.23.1.20121113
```

Related Commands

None

14.5.2 Setenv

Command Purpose

Use this command to set Bootrom environment variables.

Command Syntax

```
setenv ( ipaddr | serverip IP_ADDR | bootcmd boot arguments )
```

Parameter	Parameter Description	Parameter Value
IP_ADDR	Local device or tftp server IP address	IPv4 Address
boot arguments	Boot from flash or tftp server	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to set Switch IP address as environment variables:

```
bootrom:> setenv ipaddr 10.10.29.48
```

This example shows how to set TFTP server IP address as environment variables:

```
bootrom:> setenv serverip 10.10.29.160
```

This example shows how to set boot command as environment variables:

```
bootrom:> setenv bootcmd boot_flash OS-ma-v3.0.1.it.r.bin
```

Related Commands

None

14.5.3 Saveenv

Command Purpose

Use the saveenv command to save the Bootrom environment variables to persistent storage.

Command Syntax

Saveenv

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to save the Bootrom environment variables:


```
bootrom:> saveenv
```

Related Commands

Printenv

14.5.4 Printenv

Command Purpose

Use the printenv command to show the U-boot environment variables.

Command Syntax

Printenv

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to show the Bootrom environment variables:

```
bootrom:> printenv
```

```
baudrate=115200
```

```
bootargs=bootimage=ulimage console=ttyS0,115200 cache-sram=0xfff00000,0x10000
```

```
bootcmd=boot_tftp switchOS-v6.2.27.r.bin
```

```
bootdelay=10
```

```
consoledev=ttyS0
```

```
ethact=eTSEC2
```

```
ethaddr=00:00:00:00:01:02
```

```
ethprime=eTSEC2
```

```
fileaddr=1000000
```

```
filesize=2126519
```

```
gatewayip=10.10.39.254
```

```
ipaddr=10.10.39.123
```

```
loadaddr=1000000
mtddevname=uboot-env
mtddevnum=0
mtdids=nand0=nand
partition=nand0,0
serial#=E132GD153002
serverip=10.10.38.160
stderr=serial
stdin=serial
stdout=serial
```

Environment size: 4720/8188 bytes

Related Commands

Setenv

14.5.5 Reset

Command Purpose

Use the reset command to perform RESET of the CPU.

Command Syntax

Reset

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to RESET the CPU in Bootrom:

```
bootrom:> reset
```

Related Commands

Saveenv

14.5.6 Ping

Command Purpose

Use the ping command to send ICMP ECHO_REQUEST to network host.

Command Syntax

ping *IP_ADDR*

Parameter	Parameter Description	Parameter Value
IP_ADDR	remote host IP address	IPv4 Address

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to use ping command in Bootrom mode:

```
Bootrom:> ping 10.10.38.160
```

```
Using FM1@DTSEC3 device
```

```
host 10.10.38.160 is alive
```

Related Commands

Saveenv

14.5.7 Ctlcs

Command Purpose

Use the ls command to list files in a directory (default is /).

Command Syntax

Ctcls

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to list files in a directory (default is /):

```
Bootrom:>ctcls
```

```
UBI: attaching mtd1 to ubi0
```

```
UBI: physical eraseblock size: 524288 bytes (512 KiB)
```

```
UBI: logical eraseblock size: 516096 bytes
```

```
UBI: smallest flash I/O unit: 4096
```

```
UBI: VID header offset: 4096 (aligned 4096)
```

```
UBI: data offset: 8192
```

```
UBI: attached mtd1 to ubi0
```

```
UBI: MTD device name: "mtd=3"
```

```
UBI: MTD device size: 896 MiB
```

```
UBI: number of good PEBs: 1792
```

```
UBI: number of bad PEBs: 0
```

```
UBI: max. allowed volumes: 128
```

```
UBI: wear-leveling threshold: 4096
```

```
UBI: number of internal volumes: 1
```

```
UBI: number of user volumes: 1
```

```
UBI: available PEBs: 80
```

```
UBI: total number of reserved PEBs: 1712
```

```
UBI: number of PEBs reserved for bad PEB handling: 17
```

```
UBI: max/mean erase counter: 805/720
```

```
UBIFS: mounted UBI device 0, volume 0, name "boot"
```

```
UBIFS: mounted read-only
```

```
UBIFS: file system size: 867041280 bytes (846720 KiB, 826 MiB, 1680 LEBs)
```

```

UBIFS: journal size:      33546240 bytes (32760 KiB, 31 MiB, 65 LEBs)
UBIFS: media format:      w4/r0 (latest is w4/r0)
UBIFS: default compressor: LZO
UBIFS: reserved for root:  5182151 bytes (5060 KiB)
                        2565  Tue Dec 04 00:40:55 2018  startup-config.conf
<LNK>                    27   Thu Nov 29 02:08:23 2018  ulmage
                        25599632 Mon Apr 02 18:25:34 2018 switchOS-e580-v6.2.27.r.bin

```

Related Commands

None

14.5.8 boot_tftp

Command Purpose

Use the boot_tftp command to boot system through the specified system image from TFTP server.

Command Syntax

boot_tftp IMAGE_NAME

Parameter	Parameter Description	Parameter Value
IMAGE_NAME	Image name of tftp server	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to boot system form TFTP server:

```
bootrom:> boot_tftp OS-ma-v3.0.1.it.r.bin
```

Related Commands

None

14.5.9 boot_tftp_nopass

Command Purpose

Use the boot_tftp_nopass command to boot system through the specified system image from TFTP server with default configuration.

Command Syntax

boot_tftp_nopass IMAGE_NAME

Parameter	Parameter Description	Parameter Value
IMAGE_NAME	Image name of tftp server	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to boot system form TFTP server:

```
bootrom:> boot_tftp_nopass OS-ma-v3.0.1.it.r.bin
```

Related Commands

None

14.5.10 boot_flash

Command Purpose

Use the boot_flash command to boot system through the specify image or default image in the flash

Command Syntax

boot_flash IMAGE_NAME

Parameter	Parameter Description	Parameter Value
IMAGE_NAME	Image name in flash	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to boot system through the specify image in the flash:

```
bootrom:> boot_flash
```

Related Commands

None

14.5.11 boot_flash_nopass**Command Purpose**

Use the boot_flash_nopass command to boot system through the specify image or default image in the flash with default configuration.

Command Syntax

boot_flash_nopass IMAGE_NAME

Parameter	Parameter Description	Parameter Value
IMAGE_NAME	Image name in flash	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to boot system through the specify image in the flash with default configuration:

```
bootrom:> boot_flash_nopass /boot/OS-ma-v3.0.1.it.r.bin
Do you want to revert to the default config file ? [Y|N|E]:Y
```

Related Commands

None

14.5.12 upgrade_uboot

Command Purpose

Use the upgrade_uboot command to upgrade the U-boot image from TFTP server.

Command Syntax

upgrade_uboot IMAGE_NAME

Parameter	Parameter Description	Parameter Value
IMAGE_NAME	Image name form tftp server	-

Command Mode

BootRom CLI

Default

None

Usage

None

Examples

This example shows how to upgrade the Bootrom image from TFTP server:


```
bootrom:> upgrade_uboot u-boot.bin
```

Related Commands

None

14.6 Bootup Diagnostic Commands

14.6.1 diagnostic bootup level

Command Purpose

Use this command to set bootup diagnostic level of next Switch reboot.

Command Syntax

diagnostic bootup level (minimal | complete)

no diagnostic bootup level

Parameter	Parameter Description	Parameter Value
minimal	Minimal bootup level test	-
complete	Complete bootup level test	-

Command Mode

Global Configuration

Default

None

Usage

None

Examples

This example shows how to set bootup diagnostic level:

```
Switch# configure terminal
```

```
Switch(config)# diagnostic bootup level minimal
```

Related Commands

None

14.6.2 show diagnostic bootup level

Command Purpose

Use this command to show bootup diagnostic level.

Command Syntax

show diagnostic bootup level

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show bootup diagnostic level:

```
Switch# show diagnostic bootup level
```

The current running bootup diag level is complete

The next running bootup diag level is complete

Related Commands

None

14.6.3 show diagnostic bootup result

Command Purpose

Use this command to show bootup diagnostic result.

Command Syntax

show diagnostic bootup result (detail |) (slot *ID* |)

Parameter	Parameter Description	Parameter Value
detail	Detailed information	-
ID	The ID of stack member.	1-29

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show bootup diagnostic level:

```
Switch# show diagnostic bootup result detail
```

```
#####
Item Name                Attribute Result Time(usec)
1    EPLD TEST           C      Pass    57
2    EEPROM0 TEST        C      Pass   101262
3    PHY TEST            C      Pass    1161
4    FAN TEST            C      Pass    4668
5    SENSOR TEST         C      Pass    5472
6    PSU TEST            C      Pass    1370
7    L2 UCAST FUNC TEST  C      Pass   40126
```

Related Commands

None

14.7 SmartConfig Commands

14.7.1 smart-config

Command Purpose

To config smartconfig function, use the smart-config command in global configuration mode.

Command Syntax

```
smart-config ( initial-switch-deployment | hostname-prefix )
```

no smart-config (initial-switch-deployment | hostname-prefix)

Parameter	Parameter Description	Parameter Value
initial-switch-deployment	Enable initial switch automatically deployment	-
hostname-prefix	Enable hostname prefix feature	-

Command Mode

Global Configuration

Default

Initial-switch-deployment and hostname-prefix is enabled.

Usage

None

Examples

The following example shows how to enable smartconfig function:

```
Switch# configure terminal
Switch(config)# smart-config initial-switch-deployment
```

The following example shows how to disable smartconfig function:

```
Switch# configure terminal
Switch(config)# no smart-config initial-switch-deployment
```

Related Commands

ip address dhcp
show smart-config config

14.7.2 show smart-config config

Command Purpose

To show configuration of smart-config, use the show smart-config configuration command in privileged EXEC mode.

Command Syntax

show smart-config config

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display configuration of smart-config:

```
Switch# show smart-config config
```

```
Smart-Config config:
```

```
initial-switch-deployment: on
```

```
hostname-prefix: on
```

```
Send log message to console: on
```

Related Commands

ip address dhcp

smart-config

Chapter 15 Network Management Commands

15.1 Network Diagnosis Commands

15.1.1 ping

Command Purpose

The switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

Normal response- The normal response (hostname is alive) occurs in 1 to 10 seconds, depending on network traffic.

Destination does not respond- If the host does not respond, a no-answer message is returned.

Unknown host- If the host does not exist, an unknown host message is returned.

Destination unreachable- If the default gateway cannot reach the specified network, a destination-unreachable message is returned.

Network or host unreachable- If there is no entry in the route table for the host or network, a network or host unreachable message is return.

Command Syntax

ping (ip | mgmt-if) *WORD*

ping (vrf *WORD* |) [-a *WORD* | -si *IFNAME* | -m *INTERVAL* | -c *COUNT* | -s *DATASIZE* | -f | -tos *TOS* | -h *TTL* | -t *TIMEOUT*] *WORD*

ping (mgmt-if | vrf *WORD* |) ipv6 [-a *WORD* | -m *INTERVAL* | -c *COUNT* | -s *DATASIZE* | -tc *TC* | -h *HL* | -t *TIMEOUT*] *WORD* (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
-a WORD	Select source IP address, the default is the IP address of the output interface	-
-si IFNAME	Set the specified interface as the source interface of ping packet	Support physical/aggregation/loopback/tunnel/vlan ports
ip	Public network IPv4 echo	-
vrf WORD	VPN Routing/Forwarding instance	Up to 15 characters
mgmt-if	Management interface	-
WORD	Ping destination IPv4 or IPv6 address or hostname	-
ipv6	Public network IPv6 echo	-
interface	Outgoing interface for LinkLocal address/host	-
IFNAME	Interface's name	Support physical/aggregation/loopback/tunnel/vlan ports
-m INTERVAL	specify interval for sending ping packets	10-10000 millisecond
-c COUNT	specify the number of ping packets	1-4294967295
-s DATASIZE	specify the data size of ping packet	20-9600 bytes
-f	specify the Don't Fragment flag in packet	-

Parameter	Parameter Description	Parameter Value
-tos TOS	Specify the packet tos value	0-255
-h TTL	specify the TTL value in ping packet	1-255
-tc TC	specify the Traffic Class value in ipv6 ping packet	0-255
-h HL	specify the Hop Limit value in ipv6 ping packet	1-255
-t TIMEOUT	specify the timeout value to wait for replay packet	0-65535 millisecond, only support multiple of 1000

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to ping a host from management interface:

```
Switch# ping mgmt-if 10.10.29.247
```

```

PING 10.10.29.247 (10.10.29.247) 56(84) bytes of data.
64 bytes from 10.10.29.247: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 10.10.29.247: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.29.247: icmp_seq=3 ttl=64 time=0.134 ms
64 bytes from 10.10.29.247: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 10.10.29.247: icmp_seq=5 ttl=64 time=0.135 ms
--- 10.10.29.247 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.121/0.143/0.194/0.025 ms

```

Related Commands

Traceroute

15.1.2 traceroute

Command Purpose

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your switches can participate as the source or destination of the traceroute privileged EXEC command and might or might not appear as a hop in the traceroute command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate switches do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN. However, if the intermediate switch is a multilayer switch that is routing a particular packet, this switch shows up as a hop in the traceroute output.

The traceroute privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

Command Syntax

```
traceroute ( ip | vrf WORD | mgmt-if | ) WORD
```

```
traceroute ( vrf WORD | ) ipv6 WORD
```

Parameter	Parameter Description	Parameter Value
-a	Select source IP address, the default is the IP address of the output interface	-
-si	Set the specified interface as the source interface of traceroute packet	-
ip	Public network IPv4 echo	-
ipv6	Public network IPv6 echo	-
vrf WORD	VPN Routing/Forwarding instance	-
mgmt-if	Management interface	-
WORD	Destination IP address or hostname	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example is sample dialog from the traceroute command using default values:

```
Switch# traceroute 1.1.1.2
```

```
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
```

```
1 1.1.1.2 (1.1.1.2) 108.129 ms 99.313 ms 94.720 ms
```

Related Commands

Ping

15.2 NTP Commands

15.2.1 ntp ace

Command Purpose

To create the Access Control Entries (ACE) of a NTP server/peer, use the ntp ace command in global configuration mode. To remove the ace, use the no form of this command.

Command Syntax

```
ntp ace ( IP_ADDR | HOSTNAME ) ( mask MASK_LENGTH | ) ( version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none )
no ntp ace ( IP_ADDR | HOSTNAME ) ( mask MASK | ) ( version | kod | ignore | noquery | nomodify | notrap | noserve | nopeer | notrust | limited | none )
```


Parameter	Parameter Description	Parameter Value
IP_ADDR	IP address of the time server or peer	IPv4 Address, exclude 127.0.0.1 & 0.0.0.0
HOSTNAME	Name of the time server or peer	Up to 256 characters
MASK_LENGTH	Specify network mask length of the address	1-32
MASK	Specify network mask of the address	In IPv4 Address format
version	Ignore these hosts if not the current NTP version	-
kod	If access is denied, send a kiss-of-death packet	-
ignore	Ignore all packets from host that match this entry	-
noquery	Ignore all NTP mode 6 and 7 packets from the source, time service is not affected	-
nomodify	Ignore all NTP mode 6 and 7 packets which attempt to modify the state of the server	-
notrap	Decline to provide mode 6 control message trap service to matching hosts	-
noserve	Ignore NTP packets whose mode is other than 6 or 7	-
nopeer	Provide stateless time service to polling hosts, but do not allocate peer memory resources	-
notrust	Treat these hosts normally in other respects, but never use them as synchronization sources	-
limited	These hosts are subject to limitation of number of clients from the same net	-
none	No limit	-

Command Mode

Global Configuration

Default

None

Usage

Use this command if you want to allow the system to synchronize with the specified server. The server will not synchronize to this machine.

Examples

The following example shows how to create an ACE for 1.1.1.1:

```
Switch# configure terminal
Switch(config)# ntp ace 1.1.1.1 version
```

Related Commands

show ntp

15.2.2 ntp authentication

Command Purpose

To enable NTP authentication, use the ntp authentication enable command. To disable the NTP authentication, use the ntp authentication disable command.

Command Syntax

ntp authentication (enable | disable)

Parameter	Parameter Description	Parameter Value
enable	Enable NTP authentication	-
disable	Disable NTP authentication	-

Command Mode

Global Configuration

Default

None

Usage

When NTP authentication is enabled, the switch will synchronize the time with NTP servers with trusted key only. For more information about trusted key, please see the ntp trustedkey command.

Examples

The following example shows how to enable NTP authentication:

```
Switch# configure terminal
Switch(config)# ntp authentication enable
```

Related Commands

show ntp

15.2.3 ntp broadcast client

Command Purpose

To configure the system to receive Network Time Protocol (NTP) broadcast packets on a specified interface, use the ntp broadcast client command in interface configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ntp broadcast client
no ntp broadcast client

Command Mode

Interface Configuration

Default

NTP broadcast client is disabled by default

Usage

Use this command to allow the system to listen to broadcast packets on an interface-by-interface. Only physical interface, vlan interface and loopback interface support this command.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ntp broadcast client
```

Related Commands

ntp broadcastdelay

15.2.4 ntp broadcastdelay

Command Purpose

To configure the change the estimated round-trip delay between the switch and the NTP broadcast server, use the ntp broadcastdelay command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ntp broadcastdelay TIME
no ntp broadcastdelay
```

Parameter	Parameter Description	Parameter Value
TIME	Delayed time interval in milliseconds, the range is 1-10000ms	1-10000 millisecond

Command Mode

Global Configuration

Default

The default value should be 3000 milli-seconds.

Usage

None

Examples

The following example shows how to change broadcast delay to 2000ms:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config)# ntp broadcastdelay 2000
```

Related Commands

ntp broadcast client

15.2.5 ntp disable

Command Purpose

To configure Disable NTP packets from being received on the interface, use the ntp disable command in interface configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ntp disable
no ntp disable
```

Command Mode

Interface Configuration

Default

By default, all interfaces receive NTP packets.

Usage

Only physical interface, vlan interface and loopback interface support this command.

Examples

In the following example, the system is configured not to receive NTP packet in interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# ntp disable
```

Related Commands

None

15.2.6 ntp key

Command Purpose

To configure value of the NTP key, use the ntp key command in global configuration mode. To remove the value of the NTP key, use the no form of this command.

Command Syntax

```
ntp key KEYID VALUE
no ntp key KEYID
```

Parameter	Parameter Description	Parameter Value
KEYID	Authentication key	1-64000
VALUE	The value of the key	Up to 128 characters

Command Mode

Global Configuration

Default

None

Usage

Use this command to create a value for a NTP key.

Examples

In the following example, the value 321 is given to the NTP key 123:

```
Switch# configure terminal
Switch(config)# ntp key 123 321
```

Related Commands

show ntp

15.2.7 ntp interface reload

Command Purpose

To reload the NTP configuration on the interfaces, use the ntp interface reload command in global configuration mode.

Command Syntax

ntp interface reload

Command Mode

Global Configuration

Default

None

Usage

Use this command to reload the NTP configuration on all the interfaces.

Examples

The following example reloads the NTP configuration on all interfaces:

```
Switch# configure terminal
Switch(config)# ntp interface reload
```

Related Commands

show ntp

15.2.8 ntp max-distance**Command Purpose**

Use ntp max-distance command to config ntp max sync distance threshold. This command used in ntp client, and ntp calculate the sync distance to each ntp server and compare it with the ntp max sync distance which configured by ntp max-distance command. If the distance calculate by ntp over the distance configured by ntp max-distance, client will not sync with this ntp server.

Command Syntax
ntp max-distance *DISTANCE*
no ntp max-distance *DISTANCE*

Parameter	Parameter Description	Parameter Value
DISTANCE	Specify the ntp max sync distance threshold in seconds, default 10s.	1-16

Command Mode

Global Configuration

Default

10

Usage

None

Examples

The following example shows the configuration of NTP:

```
Switch# configure terminal
DUT1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DUT1(config)# ntp max-distance 16
```

Related Commands

None

15.2.9 ntp peer

Command Purpose

To configure the software clock to synchronize a peer or to be synchronized by a peer, use the `ntp peer` command in global configuration mode. To disable this capability, use the `no` form of this command.

Command Syntax

```
ntp peer ( HOSTNAME | IP_ADDR ) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR }
no ntp peer ( HOSTNAME | IP_ADDR )
```

Parameter	Parameter Description	Parameter Value
HOSTNAME	Name of the time server or peer	Up to 256 characters
IP_ADDR	IP address of the time server or peer	IPv4 Address
KEY_ID	Authentication key to use when sending packets to this peer	1-64000
prefer	Makes this peer the preferred peer that provides synchronization	-
VER	Defines the Network Time Protocol (NTP) version number	1-3
IFNAME	Name of source interface	Support physical/aggregation/loopback/tunnel/vlan ports
SRC_ADDR	Source IP address	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source IP address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Using the `prefer` keyword reduces switching between peers. If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

The following example shows how to configure a switch to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IP address 192.168.22.33 using NTP version 2.:

```
Switch# configure terminal
```

```
Switch(config)# ntp peer 192.168.22.33 version 2
```

Related Commands

```
show ntp
```

15.2.10 ntp refclock

Command Purpose

To configure an external clock source for use with Network Time Protocol (NTP) services, use the `ntp refclock` command in global configuration mode. To disable support of the external time source, use the `no` form of this command.

Command Syntax

```
ntp refclock stratum NUMBER
```

```
no ntp refclock
```

Parameter	Parameter Description	Parameter Value
NUMBER	Indicates the NTP stratum number that the system will claim.	1-15

Command Mode

Global Configuration

Default

This command is disabled by default.

Usage

None

Examples

The following example shows configuration of a NTP source on a switch platform:

```
Switch# configure terminal
Switch(config)# ntp refclock stratum 1
```

Related Commands

show ntp

15.2.11 ntp server**Command Purpose**

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the ntp server command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

```
ntp server ( HOSTNAME | IP_ADDR ) { key KEY_ID | prefer | version VER } { source-interface IFNAME | source-ip SRC_ADDR }
no ntp server ( HOSTNAME | SRC_ADDR )
```

Parameter	Parameter Description	Parameter Value
HOSTNAME	Name of the time server or peer	Up to 256 characters
IP_ADDR	IP address of the time server or peer	IPv4 Address
KEY_ID	Authentication key to use when sending packets to this peer	1-64000
prefer	Makes this peer the preferred peer that provides synchronization	-
VER	Defines the Network Time Protocol (NTP) version number	1-3
IFNAME	Name of source interface	Support physical/aggregation/loopback/tunnel/vlan ports
SRC_ADDR	Source IP address	IPv4 Address

Command Mode

Global Configuration

Default

The server will not synchronize to this machine.

Usage

Use this command if you want to allow the system to synchronize with the specified server.
If the source interface or source IP address is specified, the packet transmit will use the related IP address as source address.

Examples

The following example shows how to configure a switch to allow its software clock to be synchronized with the clock by the device at IP address 172.16.22.44 using NTP version 2:

```
Switch# configure terminal
Switch(config)# ntp server 172.16.22.44 version 2
```

Related Commands

show ntp

15.2.12 ntp trustedkey

Command Purpose

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the `ntp trustedkey` command in global configuration mode. To disable authentication of the identity of the system, use the `no` form of this command.

Command Syntax

```
ntp trustedkey KEY_ID
no ntp trustedkey KEY_ID
```

Parameter	Parameter Description	Parameter Value
KEY_ID	Authentication key to use when sending packets to this peer	1-64000

Command Mode

Global Configuration

Default

None

Usage

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the `ntp key` command) that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Switch# configure terminal
Switch(config)# ntp authentication enable
Switch(config)# ntp key 42 aNiceKey
Switch(config)# ntp trustedkey 42
```

Related Commands

```
show ntp
ntp key
```

15.2.13 show ntp

Command Purpose

To display the NTP configurations, use the `show ntp` command in privileged EXEC mode.

Command Syntax

show ntp

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the NTP configurations.

Examples

The following example shows the configuration of NTP:

Switch# show ntp

Current NTP configuration:

=====

NTP access control list:

Unicast peer:

1.1.1.1

Unicast server:

2.2.2.2

Broadcast client: enabled

Authentication: enabled

Local reference clock:

enabled, stratum 10

Related Commands

ntp server

ntp peer

15.2.14 show ntp ace

Command Purpose

To display the restrict list of Access Control Entries (ACE) of a NTP server/peer, use the show ntp ace command in privileged EXEC mode.

Command Syntax

show ntp ace

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following example shows the NTP restrict list:

Switch# show ntp ace

address	mask	count	flags
0.0.0.0	0.0.0.0	55188	noquery, nomodify, notrap
6.6.6.6	255.255.255.255	73	none
127.0.0.1	255.255.255.255	1259	none

Related Commands

ntp ace

15.2.15 show ntp associations

Command Purpose

To show the status of Network Time Protocol (NTP) associations, use the show ntp associations command in privileged EXEC mode.

Command Syntax

show ntp associations

Command Mode

Privileged EXEC

Default

None

Usage

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

Examples

The following example shows the status of NTP associations:

Switch# show ntp associations

Current NTP associations:

remote	refid	st	when	poll	reach	delay	offset	disp
*6.6.6.6	127.127.1.0	6	161	256	377	0.778	-0.087	119.400

* synchronized, + candidate, # selected, x falsetick, . excess, - outlier

Related Commands

show ntp status

15.2.16 show ntp key

Command Purpose

To show the NTP keys, use the show ntp key command in privileged EXEC mode.

Command Syntax

show ntp key

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the NTP keys.

Examples

The following example shows the keys of NTP:

Switch# show ntp key

Current NTP key configuration:

Flags: * - Trusted

ID	Value

* 1	trusted_key
5	test_key

Related Commands

ntp key

15.2.17 show ntp status

Command Purpose

To show the status of the Network Time Protocol (NTP), use the show ntp status command in privileged EXEC mode.

Command Syntax

show ntp status

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following is sample output from the show ntp status command:

Switch# show ntp status

Current NTP status:

```
=====
clock is synchronized
stratum:           11
reference clock: 127.127.1.0
frequency:         0.000 ppm
precision:         2^15
reference time: d116c946.4dc2f6a7 ( 1:24:22.303 UTC Tue Mar  1 2011)
root delay:        0.000 ms
root dispersion: 449.207 ms
peer dispersion: 662.059 ms
clock offset:      0.000 ms
stability:         0.000 ppm
```

Related Commands

show ntp associations

15.2.18 show ntp statistics

Command Purpose

To show the statistics of the Network Time Protocol (NTP), use the show ntp statistics command in privileged EXEC mode.

Command Syntax

show ntp statistics

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following is sample output from the show ntp statistics command:

```
Switch# show ntp statistics
```

Current NTP I/O statistics:

```
=====
time since reset:    175834
receive buffers:     10
free receive buffers: 9
used receive buffers: 0
low water refills:   1
dropped packets:     0
ignored packets:     0
received packets:    32
packets sent:        31
packets not sent:    0
interrupts handled:  32
received by int:     32
```

Related Commands

show ntp associations

15.2.19 clear ntp statistics**Command Purpose**

To clear the statistics of the Network Time Protocol (NTP), use the clear ntp statistics command in privileged EXEC mode.

Command Syntax

```
clear ntp statistics
```

Command Mode

Privileged EXEC

Default

None

Usage

None.

Examples

The following is a sample to clear ntp statistics:

```
Switch# clear ntp statistics
```

Related Commands

show ntp statistics

15.2.20 ntp mgmt-if**Command Purpose**

To enable NTP management interface, use the `ntp mgmt-if` command. To enable management interface only, use the `only` parameter. To enable both in-band and management interface, use the `enable` parameter. To disable NTP management interface, use the `no ntp mgmt-if` command.

Command Syntax

`ntp mgmt-if ( enable | only )`
`no ntp mgmt-if`

Parameter	Parameter Description	Parameter Value
only	Only use management interface	-
enable	Both use management interface and in-band interface	-

Command Mode

Global Configuration

Default

Disable management interface by default and only use in-band interface

Usage

Use this command to enable management interface, then the ntp client will connect to the server or peer.

Examples

The following example shows only use management interface:

```
Switch# configure terminal
Switch(config)# ntp mgmt-if only
```

Related Commands

```
show ntp
ntp mgmt-if broadcast
```

15.2.21 ntp mgmt-if broadcast client

Command Purpose

To allow the system to listen to broadcast packets on management, use the `ntp mgmt-if broadcast client` command. To disable this capability, use the `no` form of this command.

Command Syntax

`ntp mgmt-if broadcast client`
`no ntp mgmt-if broadcast client`

Command Mode

Global Configuration

Default

NTP broadcast client is disabled by default

Usage

Use this command to allow the system to listen to broadcast packets on management interface.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on management interface :

```
Switch# configure terminal
Switch(config)# ntp mgmt-if broadcast client
```

Related Commands

show ntp
ntp mgmt-if

15.3 Phy Loopback Commands

15.3.1 loopback phy

Command Purpose

Use this command to configure a physical interface as phy level loopback mode. Use the no loopback command to cancel this configuration.

Command Syntax

loopback phy (internal *IFPHYSICAL* | external)

Parameter	Parameter Description	Parameter Value
internal IFPHYSICAL	Packets transmitted to the interface should be looped back to a specified physical interface without any modification. The destination physical interface	-
external	Packets received from the interface should be looped back to the interface itself without any modification	-

Command Mode

Interface Configuration

Default

None

Usage

Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.

Examples

In the following example, the physical interface is set to phy level loopback mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback phy internal eth-0-2
```

Related Commands

no loopback

15.3.2 loopback port

Command Purpose

Use this command to configure a physical interface as port level loopback mode. Use the no loopback command to cancel this configuration.

Command Syntax

loopback port (mac-address swap |)

Parameter	Parameter Description	Parameter Value
mac-address swap	If this flieed is entered, the packet's SMAC incoming from port level loopback interface will be swapped with its DMAC, and the FCS will be updated	-

Command Mode

Interface Configuration

Default

None

Usage

Only one type of loopback can be applied on a physical interface. A new configuration should replace the old configuration.

Examples

In the following example, the physical interface is set to port level loopback mode:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback port
```

Related Commands

no loopback

15.3.3 no loopback**Command Purpose**

Use this command to cancel a physical interface from phy level or port level loopback to normal interface.

Command Syntax

no loopback

Command Mode

Interface Configuration

Default

None

Usage

Phy or port level loopback can be canceled by this command.

Examples

In the following example, port level loopback is canceled by this command:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# loopback port
Switch(config-if)# no loopback
```

Related Commands

loopback phy
loopback port

15.3.4 show phy loopback

Command Purpose

Use this command to show the configuration of phy loopback.

Command Syntax

show phy loopback

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows how to show the configuration:

Switch# show phy loopback

Interface	Type	DestIntf	SwapMac
eth-0-1	port	-	no
eth-0-2	port	-	yes
eth-0-3	external	-	-
eth-0-4	internal	eth-0-5	-

Related Commands

loopback phy
loopback port

15.3.5 l2 ping

Command Purpose

Use this command to ping specified DMAC from specified physical interface, using protocol packet with ethertype 0x9009.

Command Syntax

l2 ping *HHHH.HHHH.HHHH* interface *IFPHYSICAL* ({ vlan *VLAN_ID* | interval *INTERVAL* | timeout *TIMEOUT* | count *COUNT* | size *SIZE* } |)

Parameter	Parameter Description	Parameter Value
HHHH.HHHH.HHHH	The DMAC to ping	MAC Address in HHHH.HHHH.HHHH format
interface IFPHYSICAL	The interface to ping from	Support physical ports
VLAN_ID	The vlan id of the protocol ping packet	1-4094
INTERVAL	The interval time between two ping action, second	1-65535
TIMEOUT	The time wait for a ping action, second	1-65535
COUNT	Total ping times	1-65535

Parameter	Parameter Description	Parameter Value
SIZE	The size of the protocol ping packet	64-1518

Command Mode

Privileged EXEC

Default

The ping protocol packet is without vlan tag by default.
The default interval ping time is 200 milliseconds.
The default count is 5.
The default size of the ping protocol packet is 64.

Usage

The ping action can be canceled by "Ctrl + C".

Examples

The following example shows how to ping a specified destination mac.:

```
Switch# l2 ping 0000.0000.0001 interface eth-0-1 vlan 101 interval 200 timeout 1000 count 10 size 1500
```

Related Commands

l2 ping response

15.3.6 l2 ping response**Command Purpose**

Use this command to enable l2 ping response globally. Use the no form of this command to disable it.

Command Syntax

l2 ping response enable

no l2 ping response enable

Command Mode

Interface Configuration

Default

None

Usage

If l2 ping response is not enabled, the l2 ping request packet should be dropped.

Examples

In the following example shows how to enable l2 ping response on interface:

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# l2 ping response enable
```

Related Commands

l2 ping
show l2ping response

15.3.7 show l2ping response

Command Purpose

Use this command to show the configuration of l2 ping.

Command Syntax

show l2ping response

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows how to use this command:

Switch# show l2 ping response

Interface	L2pingResp
eth-0-7	Enable
eth-0-8	Enable

Related Commands

l2 ping response

15.3.8 show l2ping state**Command Purpose****Command Syntax**

show l2ping state

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows the status of l2ping:

Switch# show l2ping response

L2 ping state.

Total count	Interval	Timeout	VlanId	Packet size	Sequence
100	1515010				

10 packet(s) transmitted, 0 received, 100 % packet loss

Related Commands

None

15.3.9 l2 ping stop

Command Purpose

Command Syntax

l2 ping stop

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows how to stop L2 ping:
Switch# l2 ping stop

Related Commands

None

15.3.10 l2 ping forward enable

Command Purpose

Command Syntax

l2 ping forward enable

no l2 ping forward enable

Command Mode

Interface Configuration

Default

Enable

Usage

None

Examples

In the following example shows how to enable l2 ping forward on interface:
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# l2 ping forward enable

Related Commands

None

15.3.11 debug l2ping

Command Purpose

Use this command to enable debugging l2 ping.

Command Syntax

debug l2ping (all | packet | send | receive | response)
no debug l2ping (all | packet | send | receive | response)

Parameter	Parameter Description	Parameter Value
all	All l2ping debug	-
packet	Packet	-
send	Send packets	-
receive	Receive packets	-
response	Response Log	-

Command Mode

Privileged EXEC

Default

All these three debugging types is off.

Usage

If packet, send, or receive debugging is on, the corresponding message will be printed.

Examples

In the following example shows how to use this command:

```
Switch# debug l2ping all
```

Related Commands

l2 ping response

15.3.12 show debugging l2ping

Command Purpose

Use this command to show the status of l2ping debugging

Command Syntax

show debugging l2ping

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

In the following example shows the status of l2ping debugging:

```
Switch# show debugging l2ping
```

```
L2ping debugging status:
  l2ping packet debugging is on
  l2ping receive debugging is on
```

```
l2ping send debugging is on
l2ping response debugging is on
```

Related Commands

l2 ping response

15.4 RMON Commands

15.4.1 rmon collection stats

Command Purpose

Use this command to enable RMON statistic collection on the interface

Command Syntax

```
rmon collection stats ID ( owner OWNER | )
no rmon collection stats ID
```

Parameter	Parameter Description	Parameter Value
ID	Specify the RMON group of statistics	1-65535
owner OWNER	The owner identity of the statistic.(optional)	Up to 15 characters

Command Mode

Interface Configuration

Default

None

Usage

To create one statistic only on a certain interface

Examples

This example shows how to collect RMON statistics for the owner test:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon collection stats 1 owner test
```

Related Commands

show rmon statistics

15.4.2 rmon collection history

Command Purpose

Use this command to enable RMON history collection for the specified number of buckets and time period

Command Syntax

```
rmon collection history INDEX ( buckets NUMBER | ) ( interval INTERVAL | ) ( owner OWNER | )
no rmon collection history INDEX
```

Parameter	Parameter Description	Parameter Value
INDEX	Specify the maximum number of buckets desired for the RMON Specify the maximum number of buckets desired for the RMON Collection history group of statistics.	1-65535

Parameter	Parameter Description	Parameter Value
buckets NUMBER	Specify the maximum number of buckets desired for the RMON collection history group of statistics.	1-65535
interval INTERVAL	Specify the number of seconds in each polling cycle.	1-3600
owner OWNER	The owner identity of history group (optional)	Up to 15 characters

Command Mode

Interface Configuration

Default

None

Usage

Use this command to enable a history statistics on a certain interface.

Examples

This example shows how to enable history RMON statistics on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon collection history 1 buckets 1000 interval 100 owner test
```

Related Commands

show rmon history

15.4.3 rmon event**Command Purpose**

Use this command to add an event to RMON event table

Command Syntax

```
rmon event INDEX ( log | ) ( trap TRAP | ) ( description DESCRIPTION | ) ( owner OWNER | )
no rmon event Index
```

Parameter	Parameter Description	Parameter Value
INDEX	Event index.	1-65535
log	Generate a RMON log when event is triggered	-
trap TRAP	Trap community	Up to 127 characters
description DESCRIPTION	Specify the description string for the event (default is RMON_SNMP) Specify the description string for the event (default is RMON_SNMP)	Up to 127 characters
owner OWNER	The owner name (default is RMON_SNMP)	Up to 15 characters

Command Mode

Global Configuration

Default

None

Usage

Create an event is for RMON alarm. Permit event special triggered operate. Log can be sent by trap.

Examples

This example shows how to create an event:

```
Switch# configure terminal
Switch(config)# rmon event 1 log trap public description reach_max owner test
```

Related Commands

show rmon event

15.4.4 rmon alarm

Command Purpose

Use this command to set an alarm on a MIB object.

Command Syntax

```
rmon alarm INDEX OID interval INTERVAL ( delta | absolute ) rising-threshold RTHRE ( event numbs | ) falling-threshold FTHRE ( event
NUMBER | ) ( owner OWNER | )
no rmon alarm Index
```

Parameter	Parameter Description	Parameter Value
INDEX	Alarm index.	1-65535
OID	Variable for setting alarm(etherStatsEntry.m.n)	MIB OID
INTERVAL	Specify the time in seconds the alarm monitors the MIB object(seconds).	1-65535
delta	Specify the delta keyword to test the change between samples of a MIB variable	-
absolute	Specify the absolute keyword to test each MIB variable directly	-
rising-threshold RTHRE	Alarm rising threshold.	-2147483648 - 2147483646
event numbs	Specify the event number to trigger when the falling threshold	1-65535
falling-threshold FTHRE	Alarm falling threshold.	-2147483648-2147483646
event NUMBER	Specify the event number to trigger when the falling threshold	1-65535
owner OWNER	exceeds its limit.	Up to 15 characters

Command Mode

Global Configuration

Default

None

Usage

We need to create events for rising threshold and falling threshold first before we create an alarm for a mib. Also the statistics need to be created on an interface, because we only support to set alarm monitor on etherStatsEntry.

Examples

This example shows how to set an alarm:

```
Switch# configure terminal
```

```
Switch(config)# rmon alarm 1 etherStatsEntry.3.1 interval 10 delta rising-threshold 1000 event 1 falling-threshold 5 event 1 owner test
```

Related Commands

None

15.4.5 show rmon statistics

Command Purpose

Use this command to show rmon statistics.

Command Syntax

show rmon statistics (*ID* |)

Parameter	Parameter Description	Parameter Value
ID	Statistics index	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

Show the interface statistics which collect by RMON

Examples

This example shows how to show rmon statistics:

```
Switch# show rmon statistics
```

```
Rmon collection index 1
  Statistics ifindex = 1, Owner: RMON_SNMP
  Input packets 0, octets 0, dropped 0
  Broadcast packets 0, multicast packets 0, CRC alignment errors 0, collisions 0
  Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
  # of packets received of length (in octets):
  64: 0, 65-127: 0, 128-255: 0
  256-511: 0, 512-1023: 0, 1024-max: 0
```

Related Commands

None

15.4.6 show rmon history

Command Purpose

Use this command to show rmon history statistics.

Command Syntax

show rmon history (*ID* |)

Parameter	Parameter Description	Parameter Value
ID	History index	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

Show the interface history statistics which collect by RMON

Examples

This example shows how to show rmon history statistics:

Switch# show rmon history

```
History index = 1
  Data source ifindex = 1
  Buckets requested = 1000
  Buckets granted = 1000
  Interval = 100
  Owner: test
  Sample # 1 Begin at 00:30:07
    Received 00 octets, 00 packets
    00 broadcast and 00 multicast packets
    00 undersized and 00 oversized packets
    00 fragments and 00 jabbers
    00 CRC alignment errors and 00 collisions.
    # of dropped packet events is 00
    Network utilization is estimated at 0
  Sample # 2 Begin at 00:31:47
    Received 00 octets, 00 packets
    00 broadcast and 00 multicast packets
    00 undersized and 00 oversized packets
    00 fragments and 00 jabbers
    00 CRC alignment errors and 00 collisions.
    # of dropped packet events is 00
    Network utilization is estimated at 0
  Sample # 3 Begin at 00:33:27
    Received 00 octets, 00 packets
    00 broadcast and 00 multicast packets
    00 undersized and 00 oversized packets
    00 fragments and 00 jabbers
    00 CRC alignment errors and 00 collisions.
    # of dropped packet events is 00
    Network utilization is estimated at 0
```

Related Commands

None

15.4.7 show rmon event**Command Purpose**

Use this command to show rmon event.

Command Syntax

show rmon event (ID |)

Parameter	Parameter Description	Parameter Value
ID	Event index.	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

Show rmon events information

Examples

This example shows how to show rmon event:
Switch# show rmon event

```
event Index = 1
  Description: RMON_SNMP
  Event type Log & Trap
  Event community name public
  Last Time Sent = 00:00:00
  Owner test
```

Related Commands

None

15.4.8 show rmon alarm**Command Purpose**

Use this command to show rmon alarm

Command Syntax

show rmon alarm (*ID* |)

Parameter	Parameter Description	Parameter Value
ID	Alarm index.	1-65535

Command Mode

Privileged EXEC

Default

None

Usage

Show rmon alarm information

Examples

This example shows how to show rmon alarm:
Switch# show rmon alarm

```
alarm Index = 1
alarm status = VALID
  alarm Interval = 3600
  alarm Type is Delta
  alarm Value = 00
  alarm Rising Threshold = 100
  alarm Rising Event = 1
```

```
alarm Falling Threshold = 10
alarm Falling Event = 1
alarm Owner is test
```

Related Commands

None

15.4.9 rmon clear counters**Command Purpose**

Use this command to clear rmon counters.

Command Syntax**Command Mode**

Interface Configuration

Default

None

Usage

Clear counters on a interface

Examples

This example shows how to clear rmon counters:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# rmon clear counters
```

Related Commands

None

15.4.10 debug rmon**Command Purpose**

Use this command to open rmon debug.

Command Syntax

```
debug rmon
no rmon debug
```

Command Mode

Privileged EXEC

Default

None

Usage

Open rmon debug

Examples

This example shows how to open rmon debug:

```
Switch# debug rmon
```

Related Commands

None

15.5 SNMP Commands

15.5.1 snmp-server access

Command Purpose

To set the access security of MIB view, use the `snmp-server access` command in global configuration mode. To remove the access security of MIB view, use the `no` form of this command.

Command Syntax

```
snmp-server access GROUP_NAME security-model usm ( noauth | auth | priv ) ( { read READ | write WRITE | notify NOTIFY | context CONTEXT
( prefix | exact | ) } )
no snmp-server access GROUP_NAME security-model usm ( noauth | auth | priv ) ( context CONTEXT | )
```

Parameter	Parameter Description	Parameter Value
GROUP_NAME	Name of the group	Up to 31 characters
security-model	Define the security model of the group	-
usm	SNMPv3 usm security model	-
auth	Specifies authentication of a packet without encrypting it	-
noauth	Specifies no authentication of a packet	-
priv	Specifies authentication of a packet with encryption	-
context CONTEXT	(Optional) Specifies the SNMP context to associate with this SNMP group and its views.	Up to 31 characters
prefix	The context only match the prefix	-
exact	The context should match the whole part	-
READ	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent	Up to 31 characters
WRITE	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.	Up to 31 characters
NOTIFY	(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap	Up to 31 characters

Command Mode

Global Configuration

Default

No SNMP access group is defined

Usage

The command is used to create a access security for MIB view.

Examples

The following is sample output from the `snmp-server access` command:

```
Switch# configure terminal
Switch(config)# snmp-server access manage security-model usm auth write _all_ read _all_
```

Related Commands

show snmp-server access

15.5.2 snmp-server community

Command Purpose

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the `snmp-server community` command in global configuration mode. To remove the specified community string, use the `no` form of this command.

Command Syntax

`snmp-server community` *STRING* (`read-only` | `read-write`) (`view` *NAME* |)
`no snmp-server community` string

Parameter	Parameter Description	Parameter Value
STRING	Community string that consists of 1 to 256 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string	A string with 1-256 characters
read-only	Specifies read-only access. Authorized management stations can retrieve only MIB objects	-
read-write	Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects	-
view NAME	Specifies a previously defined view. The view defines the objects available to the SNMP community	Up to 31 characters

Command Mode

Global Configuration

Default

No SNMP community string is defined

Usage

The `no snmp-server` command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

Examples

The following example shows how to set the read/write community string to newstring.:

```
Switch# configure terminal
Switch(config)# snmp-server community newstring read-write
```

Related Commands

snmp-server enable

15.5.3 snmp-server context

Command Purpose

To create a Simple Network Management Protocol (SNMP) context, use the `snmp-server context` command in global configuration mode. To delete an SNMP context, use the `no` form of this command.

Command Syntax

snmp-server context *CONTEXT*
no snmp-server context *CONTEXT*

Parameter	Parameter Description	Parameter Value
CONTEXT	Name of the SNMP context being created	Up to 31 characters

Command Mode

Global Configuration

Default

No SNMP contexts are configured

Usage

When you use the no snmp-server context command, all SNMP instances in that context are deleted.

Examples

The following is sample output from the snmp-server context command:

```
Switch# configure terminal
Switch(config)# snmp-server context contextA
```

Related Commands

show snmp-server context

15.5.4 snmp-server enable

Command Purpose

To enable the SNMP function, use the snmp-server enable command in global configuration mode. To disable the SNMP function, use the no form of this command.

Command Syntax

snmp-server enable
no snmp-server enable

Command Mode

Global Configuration

Default

SNMP function is disabled

Usage

The command is used to enable or disable snmp global.

Examples

The following is sample output from the snmp-server enable command:

```
Switch# configure terminal
Switch(config)# snmp-server enable
```

Related Commands

show snmp

15.5.5 snmp-server engineID

Command Purpose

To specify the Simple Network Management Protocol (SNMP) engine ID on the local device, use the `snmp-server engineID` command in global configuration mode. To remove the configured engine ID, use the `no` form of this command.

Command Syntax

`snmp-server engineID STRING`
`no snmp-server engineID`

Parameter	Parameter Description	Parameter Value
STRING	A string identifies the engine ID	String of a maximum of 64 characters that identifies the engine ID

Command Mode

Global Configuration

Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the `show snmp-server engineID` command.

Usage

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do not need to specify an engine ID for the device. For further details on the SNMP engine ID, see RFC 2571.

Examples

The following is sample output from the `snmp-server engineID` command:

```
Switch# configure terminal
Switch(config)# snmp-server engineID 30383038303830383038
```

Related Commands

`show snmp-server engineID`

15.5.6 snmp-server group

Command Purpose

To configure a new Simple Network Management Protocol (SNMP) group, use the `snmp-server group` command in global configuration mode. To remove a specified SNMP group, use the `no` form of this command.

Command Syntax

`snmp-server group GROUP_NAME user USER_NAME security-model usm`
`no snmp-server group GROUP_NAME user user-name security-model usm`

Parameter	Parameter Description	Parameter Value
GROUP_NAME	Name of the group	Up to 31 characters
USER_NAME	Name of the user in that group	Up to 31 characters
security-model	Define the group security model	-
usm	SNMPv3 usm model	-

Command Mode

Global Configuration

Default

No SNMP server groups are configured.

Usage

This command is used to add a new SNMP server group.

Examples

The following is sample output from the snmp-server group command:

```
Switch# configure terminal
Switch(config)# snmp-server group SampleA user User1 security-model usm
```

Related Commands

show snmp-server group

15.5.7 snmp-server notify

Command Purpose

To set the notification of traps for Simple Network Management Protocol (SNMP), use the snmp-server notify command in global configuration mode. To restore to the default value, use the no form of this command.

Command Syntax

```
snmp-server notify notify-name tag tag-name ( inform | trap | )
no snmp-server notify notify-name
```

Parameter	Parameter Description	Parameter Value
NOTIFY_NAME	Name of the notification	Up to 31 characters
TAG_NAME	Name of the tag	Up to 32 characters
inform	Set notify type(default is trap) to INFOR	-
trap	Set notify type(default is trap) to TRAP	-

Command Mode

Global Configuration

Default

No SNMP notify names are configured

Usage

This command is used to send events with the notification type of error to the SNMP server.

Examples

The following is sample output from the snmp-server notify command:

```
Switch# configure terminal
Switch(config)# snmp-server notify note tag tt
```

Related Commands

show snmp-server notify

15.5.8 snmp-server system-contact

Command Purpose

To set the system contact (sysContact) string, use the snmp-server system-contact command in global configuration mode. To remove the system contact information, use the no form of this command.

Command Syntax

snmp-server system-contact *TEXT*
no snmp-server system-contact

Parameter	Parameter Description	Parameter Value
TEXT	String that describes the system contact information	Up to 255 characters

Command Mode

Global Configuration

Default

No system contact string is set

Usage

This command is used to set the system contact of the SNMP agent so that these descriptions can be accessed through the configuration file.

Examples

The following is an example of a system contact string:

```
Switch# configure terminal
Switch(config)# snmp-server system-contact admin@example.com
```

Related Commands

snmp-server system-location

15.5.9 snmp-server system-location

Command Purpose

To set the system location string, use the snmp-server system-location command in global configuration mode. To remove the location string, use the no form of this command.

Command Syntax

snmp-server system-location *TEXT*
no snmp-server system-location

Parameter	Parameter Description	Parameter Value
TEXT	String that describes the system contact information	Up to 255 characters

Command Mode

Global Configuration

Default

No system location string is set

Usage

This command is used to set the system location of the SNMP agent so that these descriptions can be accessed through the configuration file.

Examples

The following is an example of a system location string:

```
Switch# configure terminal
Switch(config)# snmp-server system-location Sample Place
```

Related Commands

snmp-server system-contact

15.5.10 snmp-server target-address

Command Purpose

To specify the recipient of a Simple Network Management Protocol (SNMP) notification message, use the `snmp-server trap target-address` command in global configuration mode. To remove the specified host from the configuration, use the `no` form of this command.

Command Syntax

```
snmp-server target-address NAME param PARAM ( IPV4_ADDR | IPV6_ADDR ) ( { udpport UDP_PORT | timeout TIMEOUT | retries RETRY } | ) ( taglist LINE | )
```

```
snmp-server target-address WORD param WORD mgmt-if IPV4_ADDR ( { udpport UDP_PORT | timeout TIMEOUT | retries RETRY } | ) ( taglist LINE | )
```

```
no snmp-server target-address WORD ( mgmt-if | )
```

Parameter	Parameter Description	Parameter Value
NAME	The name of the target address	Up to 31 characters
PARAM	Define a param name which help to find target params table	Up to 31 characters
mgmt-if	Management port	-
IPV4_ADDR	IPv4 address	IPv4 Address
IPV6_ADDR	IPv6 address	IPv6 Address
udpport port	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162	0-65535
timeout number	(Optional) The timeout value, the default value is 1500 millisecond	0-65535 millisecond
retries number	(Optional) The retry time, the default value is 3	0-255
taglist LINE	(Optional) The name of the taglist (128 tags are supported).split by blank.max length is 255 character	Up to 255 characters

Command Mode

Global Configuration

Default

No snmp server is configured.

Usage

This command is used to configure a remote manager's IP address.

This command is used for SNMP v3.

Examples

The following is sample output from the `snmp-server target-address` command:

```
Switch# configure terminal
```

```
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag
```

Related Commands

```
show snmp-server target-address
```

15.5.11 snmp-server target-params

Command Purpose

To configure the parameters of the host to accept SNMP request message in global configuration mode. To remove the host's parameters, use the no form of the command.

Command Syntax

snmp-server target-params PARAM user USER_NAME security-model v3 message-processing v3 (noauth | auth | priv)
no snmp-server target-params USER_NAME

Parameter	Parameter Description	Parameter Value
PARAM	Define a param name which help to find target params table	Up to 31 characters
USER_NAME	Name of user	Up to 31 characters
noauth	Specifies no authentication of a packet	-
auth	Specifies authentication of a packet without encrypting it	-
priv	Specifies authentication of a packet with encryption	-

Command Mode

Global Configuration

Default

No snmp params is configured

Usage

This command is used for SNMP v3.

Examples

The following example shows how to set p1 parameters:

Switch# configure terminal

Switch(config)# snmp-server target-params p1 user u1 security-model v3 message-processing v3 auth

Related Commands

show snmp-server target-params

15.5.12 snmp-server trap enable

Command Purpose

To enable all Simple Network Management Protocol (SNMP) notification types that are available on your system, use the snmp-server trap enable command in global configuration mode. To disable all available SNMP notifications, use the no form of this command.

Command Syntax

snmp-server trap enable notification-type

no snmp-server trap enable notification-type

Parameter	Parameter Description	Parameter Value
notification-type	Type of notification to enable or disable. If the all argument is specified, all notifications available on your device are enabled or disabled (if the no form is used)	all/coldstart/ipsla/linkdown/linkup/loopback-detect/ptp/syncce/system/warmstart

Command Mode

Global Configuration

Default

No notifications controlled by this command are sent

Usage

The snmp-server trap enable command is used in conjunction with the snmp-server trap target-address command. Use the snmp-server trap target-address command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one snmp-server trap target-address command.

Examples

The following is sample output from the snmp-server trap enable command:

```
Switch# configure terminal
Switch(config)# snmp-server trap enable all
```

Related Commands

snmp-server trap target-address

15.5.13 snmp-server trap delay

Command Purpose

To delay snmp-server trap send, use the snmp-server trap delay command in global configuration mode. To disable trap delay, use the no form of this command.

Command Syntax

```
snmp-server trap delay ( linkup | linkdown ) TIMER
no snmp-server trap delay ( linkup | linkdown )
```

Parameter	Parameter Description	Parameter Value
TIMER	The time to delay up/down. Unit:100 millisecond	1-100

Command Mode

Global Configuration

Default

No delay is enabled

Usage

The link down and up trap will send immediately while link state change. The command can configure a delay time for link status trap. The unit is 100ms.

Examples

The following is sample output from the snmp-server trap enable command:

```
Switch# configure terminal
Switch(config)# snmp-server trap delay linkup 10
```

Related Commands

snmp-server trap target-address

15.5.14 snmp-server trap target-address

Command Purpose

To configure a remote trap manager's IP address, use the snmp-server target-address command in global configuration mode. To remove the configuration, use the no form of this command.

Command Syntax

snmp-server trap target-address (mgmt-if | vrf *VRF_NAME* |) (*IPv4_ADDR* | *IPv6_ADDR*) community *COMMUNITY* (udpport *UDP_PORT* |)
no snmp-server trap target-address (mgmt-if | vrf *VRF_NAME* |) (*IPv4_ADDR* | *IPv6_ADDR*) community *COMMUNITY* (udpport *UDP_PORT* |)

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf <i>VRF_NAME</i>	VRF name	Up to 15 characters
<i>IPv4_ADDR</i>	IPv4 address	IPv4 Address
<i>IPv6_ADDR</i>	IPv6 address	IPv6 Address
COMMUNITY	Password-like community string sent with the notification operation	Up to 255 characters
UDP_PORT	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162	1-65535

Command Mode

Global Configuration

Default

The router does not send any trap messages.

Usage

This command is used to specify the server target address to which the trap is sent.

Examples

The following is sample output from the snmp-server trap target-address command:

```
Switch# configure terminal
Switch(config)# snmp-server trap target-address mgmt-if 192.168.1.100 community test udpport 6000
```

Related Commands

snmp-server trap enable

15.5.15 snmp-server inform target-address

Command Purpose

To specify the recipient of a Simple Network Management Protocol (SNMP) inform message, use the snmp-server inform target-address command in global configuration mode. To remove the specified host from the configuration, use the no form of this command.

Command Syntax

```
snmp-server inform target-address ( mgmt-if | vrf VRF_NAME | ) ( IPV4_ADDR | IPV6_ADDR ) community COMMUNITY ( udpport UDP_PORT | )
no snmp-server inform target-address ( mgmt-if | vrf VRF_NAME | ) ( IPV4_ADDR | IPV6_ADDR ) community COMMUNITY ( udpport UDP_PORT | )
```

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
vrf VRF_NAME	VRF name	Up to 15 characters
IPV4_ADDR	IPv4 address	IPv4 Address
IPV6_ADDR	IPv6 address	IPv6 Address
COMMUNITY	Password-like community string sent with the notification operation	Up to 255 characters
UDP_PORT	(Optional) Specifies that SNMP notifications or informs are to be sent to an SNMP manager. The default port is 162	1-65535

Command Mode

Global Configuration

Default

The router does not send any inform messages

Usage

This command is used to specify the server target address to which the inform is sent.

Examples

The following is sample output from the snmp-server inform target-address command:

```
Switch# configure terminal
```

```
Switch(config)# snmp-server inform target-address mgmt-if 192.168.1.100 community test udpport 6000
```

Related Commands

None

15.5.16 snmp-server inform

Command Purpose

Use this command in global to configure Simple Network Management Protocol (SNMP) inform message parameters, include timeout and retries. Use the no form of this command to remove inform parameters.

Command Syntax

```
snmp-server inform ( { retries RETRY | timeout TIMEOUT } )
```

```
no snmp-server inform ( retries | timeout | )
```

Parameter	Parameter Description	Parameter Value
RETRY	The retry time, the default value is 3	0-10
TIMEOUT	The timeout value, the default value is 15 second	1-1800s

Command Mode

Global Configuration

Default

No snmp inform parameters is configured

Usage

This command is used for SNMP v2.

Examples

The following example shows how to configure inform message parameters:

```
Switch(config)# snmp-server inform timeout 10 retries 5
```

Related Commands

None

15.5.17 snmp-server usm-user**Command Purpose**

To specify the recipient of a Simple Network Management Protocol (SNMP) notification message, use the `snmp-server trap target-address` command in global configuration mode. To remove the specified host from the configuration, use the `no` form of this command.

Command Syntax

```
snmp-server usm-user USERNAME ( remote REMOTE ) ( authentication ( md5 | sha ) ( 8 | ) AUTH_PWD ( privacy ( aes | des ) ( 8 | ) PRIVACY_PWD ) ) )
```

```
no snmp-server usm-user USERNAME
```

Parameter	Parameter Description	Parameter Value
USERNAME	Name of the user on the host that connects to the agent	Up to 31 characters
remote REMOTE	(Optional) Specifies a remote SNMP entity to which the user belongs	A string with 10-64 characters
authentication	(Optional) Specifies which authentication level should be used	-
md5	(Optional) Specifies the HMAC-MD5 authentication level	-
sha	(Optional) Specifies the HMAC-SHA authentication level	-
AUTH_PWD	(Optional) String that enables the agent to receive packets from the host	Up to 63 characters
privacy	(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security	-
aes	(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption	-
des	(Optional) Specifies the use of the Digital Encryption Standard (DES) algorithm for encryption	-
8	Specifies a HIDDEN password will follow	-
PRIVACY_PWD	(Optional) String that specifies the privacy user password	Up to 63 characters

Command Mode

Global Configuration

Default

No SNMPv3 users are configured

Usage

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

Examples

The following is sample output from the snmp-server usm-user command:

```
Switch# configure terminal
Switch(config)# snmp-server usm-user user1 authentication md5 mypassword privacy des yourpassword
```

Related Commands

snmp-server engineID

15.5.18 snmp-server version

Command Purpose

To specify the support of SNMP version, use the snmp-server version command in global configuration mode. To restore to the default value, use the no form of this command.

Command Syntax

```
snmp-server version ( all | v1 | v2c | v3 )
no snmp-server version
```

Parameter	Parameter Description	Parameter Value
all	Support all versions (v1, v2c, and v3)	-
v1	Support only v1 version	-
v2c	Support only v2c version	-
v3	Support only v3 version	-

Command Mode

Global Configuration

Default

Support all SNMP versions

Usage

This command is used to set the SNMP version the switch supported.

Examples

The following is sample output from the snmp-server version command:

```
Switch# configure terminal
Switch(config)# snmp-server version all
```

Related Commands

show snmp-server version

15.5.19 snmp-server view

Command Purpose

To create or update a view entry, use the snmp-server view command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the no form of this command.

Command Syntax

snmp-server view *NAME* (included | excluded) sub-tree (mask *MASK* |)
no snmp-server view *NAME* (included | excluded) sub-tree

Parameter	Parameter Description	Parameter Value
NAME	Label for the view record that you are updating or creating. The name is used to reference the record	Up to 31 characters
included	Configures the OID (and subtree OIDs) specified in sub-tree argument to be included in the SNMP view	-
excluded	Configures the OID (and subtree OIDs) specified in sub-tree argument to be explicitly excluded from the SNMP view	-
sub-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view	-
MASK	Define the subtree mask	Up to 32 hexadecimal

Command Mode

Global Configuration

Default

No view entry exists

Usage

Other SNMP commands require an SMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Examples

The following is sample output from the snmp-server view command:

```
Switch# configure terminal
Switch(config)# snmp-server view abc excluded 1.3.6.2
```

Related Commands

show snmp-server view

15.5.20 snmp-server access-group *NAME* in

Command Purpose

To set the access group, use the snmp-server access-group command in global configuration mode. To remove the access group, use the no form of this command.

Command Syntax

snmp-server access-group *NAME* in

Parameter	Parameter Description	Parameter Value
NAME	Access-list name	Up to 40 characters
in	Inbound packets	-

Command Mode

Global Configuration

Default

No access group is defined

Usage

The command is used to apply ACL in snmp.

Examples

The following is sample output from the snmp-server access command:

```
Switch# configure terminal
Switch(config)# snmp-server access-group abc in
```

Related Commands

None

15.5.21 show snmp**Command Purpose**

To display the services information of SNMP, use the show snmp command in privileged EXEC mode.

Command Syntax

```
show snmp
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the service information of SNMP (enable or disable).

Examples

The following is sample output from the show snmp command:

```
Switch# show snmp
SNMP services: enable
```

Related Commands

snmp-server enable

15.5.22 show snmp-server access

Command Purpose

To display the ACL information of SNMP, use the show snmp-server access command in privileged EXEC mode.

Command Syntax

show snmp-server access (*GROUP_NAME* |)

Parameter	Parameter Description	Parameter Value
GROUP_NAME	Specify a group name	Up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the access information configured by command snmp-server access.

Examples

The following is sample output from the show snmp-server access command:

```
Switch# show snmp-server access gp1
```

```
Group name:      gp1
Context:         test
Security model:  usm
Security level:  auth
Context Match:   exact
Read view:       _all_
Write view:      none
Notify view:     none
Storage Type:    permanent
Row status:      active
```

Related Commands

snmp-server access

15.5.23 show snmp-server community

Command Purpose

To display the SNMP community information, use the show snmp-server community command in privileged EXEC mode.

Command Syntax

show snmp-server community

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the community information configured by command `snmp-server community`.

Examples

The following is sample output from the `show snmp-server community` command:

```
Switch# show snmp-server community
```

Community-Access	Community-String	Security-name
read-only	public	comm1
read-write	private	comm2

Related Commands

`snmp-server community`

15.5.24 show snmp-server context

Command Purpose

To display the SNMP context information, use the `show snmp-server context` command in privileged EXEC mode.

Command Syntax

`show snmp-server context`

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the context information configured by command `snmp-server context`.

Examples

The following is sample output from the `show snmp-server context` command:

```
Switch# show snmp-server context
samplecontext
```

Related Commands

`snmp-server context`

15.5.25 show snmp-server engineID

Command Purpose

To display the identification of the local Simple Network Management Protocol (SNMP) engine and all remote engines that have been configured on the router, use the `show snmp-server engineID` command in EXEC mode.

Command Syntax

`show snmp-server engineID`

Command Mode

Privileged EXEC

Default

None

Usage

An SNMP engine is a copy of SNMP that can reside on a local or remote device.

Examples

The following example specifies 0000000902000000c025808 as the local engineID:

```
Switch# show snmp-server engineID
```

```
Engine ID   : 0000000902000000c025808
```

Related Commands

snmp-server engineID

15.5.26 show snmp-server group

Command Purpose

To display the names of configured SNMP groups, the security model being used, the status of the different views, and the storage type of each group, use the show snmp-server group command in privileged EXEC mode.

Command Syntax

```
show snmp-server group ( GROUP_NAME | )
```

Parameter	Parameter Description	Parameter Value
GROUP_NAME	Specify a group name	Up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

SNMP groups are configured using the snmp-server group command.

Examples

The following is sample output from the show snmp-server group command:

```
Switch# show snmp-server group
```

Group-name	model	Security-name
a11	usm	a
a11	usm	ab

Related Commands

snmp-server group

15.5.27 show snmp-server notify

Command Purpose

To display notification information of SNMP, use the show snmp-server notify command in privileged EXEC mode.

Command Syntax

```
show snmp-server notify ( GROUP_NAME | )
```

Parameter	Parameter Description	Parameter Value
GROUP_NAME	Specify a group name	Up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the notification information configured by command `snmp-server notify`.

Examples

The following is sample output from the `show snmp-server notify` command:

```
Switch# show snmp-server notify
```

Notify-name	Notify-type
sample	trap

Related Commands

`snmp-server notify`

15.5.28 show snmp-server sys-info**Command Purpose**

To display the system information of SNMP, use the `show snmp-server sys-info` command in privileged EXEC mode.

Command Syntax

```
show snmp-server sys-info
```

Command Mode

Privileged EXEC

Default

None

Usage

The system contact can be set by using the `snmp-server system-contact` command. The system location can be set by using the `snmp-server system-location` command.

Examples

The following is sample output from the `show snmp-server sys-info` command:

```
Switch# show snmp-server sys-info
```

```
Contact:  admin@sampledomain.com
Location:  Denvor
```

Related Commands

`snmp-server system-contact`
`snmp-server system-location`

15.5.29 show snmp-server trap-receiver

Command Purpose

To display the SNMP traps receiver, use the show snmp-server trap-receiver command in privileged EXEC mode.

Command Syntax

```
show snmp-server trap-receiver
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display traps receiver information configured by command snmp-server trap target-addres.

Examples

The following is sample output from the show snmp-server trap-receiver command:

```
Switch# show snmp-server trap-receiver
```

Target-ipaddress	udpport	version	pdu-type	community
1.1.1.1	234	v2c	inform	public
1.1.1.1	234	v2c	trap	public
1.1.1.1	234	v1	trap	public

Related Commands

```
snmp-server trap target-addres
```

15.5.30 show snmp-server usm-user

Command Purpose

To display information about the configured characteristics of Simple Network Management Protocol (SNMP) users, use the show snmp-server usm-user command in privileged EXEC mode.

Command Syntax

```
show snmp-server usm-user ( USERNAME | )
```

Parameter	Parameter Description	Parameter Value
USERNAME	(Optional) Name of a specific user or users about which to display SNMP information	Up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

An SNMP user must be part of an SNMP group, as configured using the snmp-server usm-user command.

Examples

The following is sample output from the show snmp-server usm-user command:

```
Switch# show snmp-server usm-user user1
```

```
EngineID:      01234567890123456789
User Name:     user1
Auth Protocol:  md5
Priv Protocol:  des
Storage Type:   nonvolatile
Row status:     active
```

Related Commands

snmp-server usm-user

15.5.31 show snmp-server version

Command Purpose

To display the supported version of SNMP, use the show snmp-server version command in privileged EXEC mode.

Command Syntax

```
show snmp-server version
```

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display snmp version information configured by command snmp-server version.

Examples

The following is sample output from the show snmp-server version command:

```
Switch# show snmp-server version
```

```
SNMPv1/SNMPv2c/SNMPv3
```

Related Commands

snmp-server version

15.5.32 show snmp-server view

Command Purpose

To display the family name, storage type, and status of a Simple Network Management Protocol (SNMP) configuration and associated MIB, use the show snmp-server view command in privileged EXEC mode.

Command Syntax

```
show snmp-server view ( NAME | )
```

Parameter	Parameter Description	Parameter Value
NAME	Specify a view name	Up to 31 characters

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the SNMP view configuration.

Examples

The following is sample output from the show snmp-server view command:
Switch# show snmp-server view

View-name	View-type	Subtree
=====	=====	=====
abc	excluded	.1.3.6.2
all	included	.0
all	included	.1
all	included	.2
none	excluded	.0
none	excluded	.1
none	excluded	.2

Related Commands

snmp-server view

15.6 SFLOW Commands

15.6.1 sflow enable

Command Purpose

Use this command to enable or disable sFlow globally.

Command Syntax

sflow enable
no sflow enable

Command Mode

Global Configuration

Default

Disabled

Usage

Before any other sFlow command can be configured, sFlow services must be enabled globally. Use the no parameter with this command to remove all sFlow configurations and disable sFlow globally.

Examples

This example shows how to enable sFlow services globally:

```
Switch# configure terminal
Switch(config)# sflow enable
```

Related Commands

show sflow

15.6.2 sflow agent

Command Purpose

Use this command to configure sFlow agent.

Command Syntax

```
sflow agent ( ip IPV4_ADDR | ipv6 ipv6-address )  
no sflow agent ( ip | ipv6 )
```

Parameter	Parameter Description	Parameter Value
IPV4_ADDR	Agent IPv4 address	IPv4 Address
IPV6_ADDR	Agent IPv6 address	IPv6 Address

Command Mode

Global Configuration

Default

None

Usage

Use this command to configure IP address for sflow agent. If not configured and router-id has configured, sflow will use the valid interface with max router-id and then never change.

Examples

This example shows how to configure agent with IP address 10.0.0.254.:

```
Switch# configure terminal  
Switch(config)# sflow agent ip 10.0.0.254
```

Related Commands

show sflow

15.6.3 sflow collector

Command Purpose

Use this command to configure sFlow collector.

Command Syntax

```
sflow collector ( IPV4_ADDR | ipv6-address ) ( UDP_PORT | )  
no sflow collector ( IPV4_ADDR | ipv6-address ) ( <UDP_PORT | )
```

Parameter	Parameter Description	Parameter Value
IPV4_ADDR	Collector IPv4 address	IPv4 Address
IPV6_ADDR	Collector IPv6 address	IPv6 Address
UDP_PORT	Collector UDP port number, default is 6343	1-65535

Command Mode

Global Configuration

Default

None

Usage

Use this command to add a collector by specifying the combination of IP address and UDP port. Only up to two unique combinations can be allowed to add. Use the no parameter with this command to delete collector.

Examples

This example shows how to add a collector with IP address 10.0.0.254 and UDP port 3000.:

```
Switch# configure terminal
Switch(config)# sflow collector 10.0.0.254 3000
```

Related Commands

show sflow

15.6.4 sflow counter interval

Command Purpose

Use this command to configure sFlow polling-interval for counter sample.

Command Syntax

```
sflow counter interval INTERVAL
no sflow counter interval
```

Parameter	Parameter Description	Parameter Value
INTERVAL	Interval value in second	1-2000 second

Command Mode

Global Configuration

Default

20 seconds

Usage

Use this command to set sFlow polling-interval for counter sample. Use the no parameter with this command to restore to the default value. Default interval value is 20 seconds.

Examples

This example shows how to set sFlow polling-interval to 10 second:

```
Switch# configure terminal
Switch(config)# sflow counter interval 10
```

Related Commands

show sflow

15.6.5 sflow counter-sampling enable

Command Purpose

Use this command to enable or disable counter sampling on specified port.

Command Syntax

```
sflow counter-sampling enable
no sflow counter-sampling enable
```

Command Mode

Interface Configuration

Default

Disabled

Usage

Use this command to enable counter sampling on specified port. Use the no parameter with this command to disable counter sampling. By default, sFlow counter sampling is disabled in all ports. This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

Examples

This example shows how to enable sFlow counter sampling on interface eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow counter-sampling enable
```

Related Commands

show sflow

15.6.6 sflow flow-sampling rate

Command Purpose

Use this command to configure flow sampling rate.

Command Syntax

sflow flow-sampling rate *RATE*
no sflow flow-sampling rate

Parameter	Parameter Description	Parameter Value
RATE	Sample rate value	must be a power of 2, the range is 32-1048576

Command Mode

Interface Configuration

Default

8192

Usage

Use this command to set sFlow packet sampling rate. Use no parameter with this command to set default sampling rate. Default sampling rate value is 8192.

sFlow uses CPU resources to collect samples and send samples to the collector. If a low sampling rate is set, CPU utilization can become high. To protect CPU from overwhelming, exceeded flow samples would be dropped. If a sampling rate less than default value is configured, a prompt will be given to info the potential of involving a high CPU utilization.

This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

Examples

This example shows how to set the sFlow sampling rate to 2048 on eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling rate 2048
```

% Warning: sFlow sampling requires high CPU usage, especially with a low rate.
It is suggested not configure a rate less than default value 8192.

Related Commands

show sflow

15.6.7 sflow flow-sampling enable

Command Purpose

Use this command to enable or disable packet sampling on individual port.

Command Syntax

sflow flow-sampling enable (input | output | both)
no sflow flow-sampling enable (input | output | both)

Command Mode

Interface Configuration

Default

Disabled

Usage

Use this command to enable ingress direction of packet sampling on individual port. Use the no parameter with this command to disable packet sampling. By default, sFlow packet sampling is disabled in all ports. This command can only be configured on a port which is not a link-agg group member. The port can be either a physical port or a link-agg port.

Examples

This example shows how to enable input packet sampling on route port eth-0-1:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# sflow flow-sampling enable input
```

Related Commands

show sflow

15.6.8 show sflow

Command Purpose

Use this command to show the running information of sflow.

Command Syntax

show sflow

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to show the running information of sflow.

Examples

This example shows how to show the sflow running information:

```
Switch# show sflow
```

```
sFlow Version: 5
sFlow Global Information:
  Agent IP address      : 0.0.0.0
  Counter Sampling Interval : 20 seconds
  Collector IP          : Not configured
sFlow Port Information:
  Port      Flow-Sample Counter  Flow-Sample Flow  Flow-Sample Direction  Rate
  -----
eth-0-1    Disable      Enable      Input            8192
```

Related Commands

```
sflow enable
sflow collector
```

15.7 LLDP Commands

15.7.1 lldp enable(global)

Command Purpose

To enable LLDP function globally, use the `lldp enable` command in global configuration mode. To disable this function, use the no form of this command.

Command Syntax

```
lldp enable
lldp disable
```

Command Mode

Global Configuration

Default

Disable

Usage

None

Examples

The following example shows how to enable LLDP globally:

```
Switch# configure terminal
Switch(config)# lldp enable
```

Related Commands

```
lldp enable (interface)
```

15.7.2 lldp enable(interface)

Command Purpose

To enable LLDP function on interface, use the `lldp enable` command in interface configuration mode. To disable this function, use the no form of this command.

Command Syntax

```
lldp enable ( txonly | txrx | rxonly )
lldp disable
```

Parameter	Parameter Description	Parameter Value
txonly	Enable lldp pdu transmission	-
txrx	Enable lldp pdu transmission and reception	-
rxonly	Enable lldp pdu reception	-

Command Mode

Interface Configuration

Default

Enable

Usage

None

Examples

The following example shows how to enable LLDP on interface:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp enable txrx
```

Related Commands

lldp enable (global)

15.7.3 lldp system-name**Command Purpose**

To configure system name for System Name TLV, use the lldp system-name command in global configuration mode. To restore the default configuration, use the no form of this command.

Command Syntax

```
lldp system-name NAME
no lldp system-name
```

Parameter	Parameter Description	Parameter Value
NAME	System Name.	A string with 1-64 characters

Command Mode

Global Configuration

Default

Default system name is used.

Usage

If no system name is configured, the default system name will be used.

Examples

The following example shows how to configure system name:

```
Switch# configure terminal
Switch(config)# lldp system-name switch
```

Related Commands

lldp enable (global)
lldp enable (interface)

15.7.4 lldp system-description

Command Purpose

To configure system description for System Description TLV, use the lldp system- description command in global configuration mode. To restore the default configuration, use the no form of this command.

Command Syntax

lldp system-description *LINE*
no lldp system-description

Parameter	Parameter Description	Parameter Value
LINE	System Description. The range is from 1 to 255 and space is allowed	A string with 1-255 characters

Command Mode

Global Configuration

Default

Default system description is used.

Usage

If no system description is configured, the default system description will be used.

Examples

The following example shows how to configure system description:

```
Switch# configure terminal  
Switch(config)# lldp system-description switch
```

Related Commands

lldp enable (global)
lldp enable (interface)

15.7.5 lldp management

Command Purpose

To configure management ip address for Management Address TLV, use the lldp management ip command in global configuration mode. To restore the default configuration, use the no form of this command.

Command Syntax

lldp management (ip *ADDRESS* | interface *IFNAME*)
no lldp management (ip | interface)

Parameter	Parameter Description	Parameter Value
ADDRESS	IPv4 address, like 1.1.1.1	IPv4 Address
IFNAME	Name of L3 interface	Support physical/aggregation/loopback/vla n/tunnel/management ports

Command Mode

Global Configuration

Default

Default management address is used.

Usage

The configured IP address has higher priority than configured interface. If both of them are not configured, system should use the loopback interface, management interface, other interface or system MAC address according to descending order of priority.

Examples

The following example shows how to configure the management IP address:

```
Switch# configure terminal
Switch(config)# lldp management ip 192.168.1.2
```

Related Commands

lldp enable (global)
lldp enable (interface)

15.7.6 lldp msg-tx-hold

Command Purpose

To configure msg-tx-hold, use the lldp msg-tx-hold command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax

lldp msg-tx-hold *NUMBER*
no lldp msg-tx-hold

Parameter	Parameter Description	Parameter Value
NUMBER	msg-tx-hold value	2-10

Command Mode

Global Configuration

Default

The default value of msg-tx-hold is 4.

Usage

None

Examples

The following example shows how to configure msg-tx-hold:

```
Switch# configure terminal
Switch(config)# lldp msg-tx-hold 3
```

Related Commands

lldp enable (global)
lldp enable (interface)

15.7.7 lldp timer msg-tx-interval

Command Purpose

To configure msg-tx-interval, use the lldp timer msg-tx-interval command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax

lldp timer msg-tx-interval *NUMBER*
no lldp timer msg-tx-interval

Parameter	Parameter Description	Parameter Value
NUMBER	msg-tx-interval value	msg-tx-hold

Command Mode

Global Configuration

Default

The default value of msg-tx-interval is 30s.

Usage

None

Examples

The following example shows how to configure msg-tx-interval:

```
Switch# configure terminal
Switch(config)# lldp timer msg-tx-interval 20
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.8 lldp timer reinit-delay

Command Purpose

To configure reinitDelay, use the lldp timer reinitDelay command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax

lldp timer reinit-delay *NUMBER*
no lldp timer reinit-delay

Parameter	Parameter Description	Parameter Value
NUMBER	reinit-delay value	1-10

Command Mode

Global Configuration

Default

The default value of reinitDelay is 2s.

Usage

None

Examples

The following example shows how to configure reinitDelay:

```
Switch# configure terminal
Switch(config)# lldp timer reinit-delay 1
```

Related Commands

lldp enable (global)
lldp enable (interface)

15.7.9 lldp timer tx-delay

Command Purpose

To configure tx-delay, use the lldp timer tx-delay command in global configuration. To restore the default configuration, use the no form of this command.

Command Syntax

lldp timer tx-delay *NUMBER*
no lldp timer tx-delay

Parameter	Parameter Description	Parameter Value
NUMBER	tx-delay value	1-8192

Command Mode

Global Configuration

Default

The default value of tx-delay is 2s.

Usage

The value of tx-delay should obey the formula: $1 \leq \text{tx-delay} \leq ((0.25) * \text{msg-tx-interval})$.

Examples

The following example shows how to configure tx-delay:

```
Switch# configure terminal
Switch(config)# lldp timer tx-delay 3
```

Related Commands

lldp enable(全局)
lldp enable(接口)

15.7.10 lldp tlv basic

Command Purpose

To select the basic tlv used in LLDP packet, use the lldp tlv basic command in interface configuration. To cancel the tlv, use the no form of this command..

Command Syntax

lldp tlv basic { port-description | system-name | system-description | system-capabilities | management-address | all }
no lldp tlv basic { port-description | system-name | system-description | system-capabilities | management-address | all }

Parameter	Parameter Description	Parameter Value
port-description	Select Port Description Tlv	-

Parameter	Parameter Description	Parameter Value
system-name	Select System Name Tlv	-
system-description	Select System Description Tlv	-
system-capabilities	Select System Capabilities Tlv	-
management-address	Select Management Address Tlv	-
all	Select All basic tlvs	-

Command Mode

Interface Configuration

Default

All basic tlvs is selected.

Usage

None

Examples

The following example shows how to select basic tlv:

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv basic system-name
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.11 lldp tlv 8021-org-specific

Command Purpose

To select the IEEE 802.1 tlvs used in LLDP packet, use the lldp tlv 8021-org-specific command in interface configuration. To cancel the tlv, use the no form of this command..

Command Syntax

lldp tlv 8021-org-specific { port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation | dcbx | all }
no lldp tlv 8021-org-specific { port-vlan | protocol-vlan | vlan-name | protocol-id | link-aggregation | dcbx | all }

Parameter	Parameter Description	Parameter Value
port-vlan	Select Port Vlan ID Tlv	-
protocol-vlan	Select Port and Protocol Vlan ID Tlv	-
vlan-name	Select Vlan Name Tlv	-
protocol-id	Select Protocol Identity Tlv	-
link-aggregation	Select Link Aggregation Tlv	-
dcbx	Select DCBX TLV	-

Parameter	Parameter Description	Parameter Value
all	Select All IEEE 802.1 tlv, exclude Link Aggregation Tlv	-

Command Mode

Interface Configuration

Default

All IEEE 802.1 tlv is selected, exclude Link Aggregation Tlv.

Usage

Link Aggregation Tlv in IEEE 802.3 tlv set is used by default.

Examples

The following example shows how to select IEEE 802.1 tlv :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv 8021-org-specific vlan-name
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.12 lldp tlv 8021-org-specific vlan-name-value**Command Purpose**

To configure the value for VLAN NAME TLV in the IEEE 802.1 tlv, use the lldp tlv 8021-org-specific vlan-name-value command in interface configuration. To cancel the configuration, use the no form of this command..

Command Syntax

lldp tlv 8021-org-specific vlan-name-value *VLAN_ID*
no lldp tlv 8021-org-specific vlan-name-value

Parameter	Parameter Description	Parameter Value
VLAN_ID	The value of Vlan ID for the VLAN NAME TLV	1-4094

Command Mode

Interface Configuration

Default

The VLAN NAME TLV will contain the information of native vlan.

Usage

None

Examples

The following example shows how to configure VLAN NAME TLV :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv 8021-org-specific vlan-name-value 2000
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.13 lldp tlv 8023-org-specific

Command Purpose

To select the IEEE 802.3 tlv used in LLDP packet, use the lldp tlv 8023-org-specific command in interface configuration. To cancel the tlv, use the no form of this command..

Command Syntax

```
lldp tlv 8023-org-specific { mac-phy-cfg | power | link-aggregation | max-frame-size | all }  
no lldp tlv 8023-org-specific { mac-phy-cfg | power | link-aggregation | max-frame-size | all }
```

Parameter	Parameter Description	Parameter Value
mac-phy-cfg	Select MAC/PHY Configuration/Status TLV	-
power	Select Power Via MDI TLV	-
link-aggregation	Select Link Aggregation TLV	-
max-frame-size	Select Maximum Frame Size TLV	-
all	Select All IEEE 802.3 tlv	-

Command Mode

Interface Configuration

Default

All IEEE 802.3 tlv is selected.

Usage

Link Aggregation TLV in IEEE 802.3 tlv set is used by default.

Examples

The following example shows how to select IEEE 802.3 tlv :

```
Switch# configure terminal  
Switch(config)# interface eth-0-1  
Switch(config-if)# lldp tlv 8023-org-specific power
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.14 lldp tlv med

Command Purpose

To select the MED tlv used in LLDP packet, use the lldp tlv med command in interface configuration. To cancel the tlv, use the no form of this command..

Command Syntax

```
lldp tlv med { network-policy | ext-power | inventory | all }  
no lldp tlv med { network-policy | ext-power | inventory | all }
```

Parameter	Parameter Description	Parameter Value
network-policy	Select Network Policy TLV	-
ext-power	Select Extend Power-Via-MDI Tlv	-
inventory	Select Inventory Tlv	-
all	Select All MED tlvs, exclude Location Identification Tlv	-

Command Mode

Interface Configuration

Default

All MED tlys is selected, exclude Location Identification Tly.

Usage

LLDP-MED Capabilities TLV will be added automatically when any other tlv in MED tlv set was selected, and canceled when no other MED tlv except itself was selected.

Examples

The following example shows how to select MED tlv :

Switch# configure terminal

```
Switch(config)# interface eth-0-1
```

```
Switch(config-if)# lldp tlv med inventory
```

Related Commands

```
lldp enable(global)
```

```
lldp enable(interface)
```

15.7.15 Ildp tlv med location-id

Command Purpose

To select and configure the MED Location-id tlv used in LLDP packet, use the `lldp tlv med location-id` command in interface configuration. To cancel the tlv, use the `no` form of this command..

Command Syntax

```
lldp tlv med location-id ( ecs-elin VALUE | civic DEV-TYPE CODE CA1-TYPE CA1-VALUE ( CA2-TYPE CA2-VALUE ( CA3-TYPE CA3-VALUE ( CA4-TYPE  
CA4-VALUE ( CA5-TYPE CA5-VALUE ( CA6-TYPE CA6-VALUE ( CA7-TYPE CA7-VALUE ( CA8-TYPE CA8-VALUE ( CA9-TYPE CA9-VALUE ( CA10-TYPE  
CA10-VALUE ) ) ) ) ) ) ) ) ) ) ) ) ) )
```

```
no lldp tlv med location-id
```

Parameter	Parameter Description	Parameter Value
ecs-elin VALUE	The ECS-ELIN address should be a telephone number	The ECS-ELIN address should be a telephone number in range [10-25]
civic DEV-TYPE	DEV-TYPE , 0 - DHCP Server, 1 - the closet network device, 2 - current devic	0-2
CODE	The two-letter ISO 3166 country code in capital ASCII letters, eg., US	CODE, The two-letter ISO 3166 country code in capital ASCII letters
CA(n)-TYPE CA(n)-VALUE	n = 1-10	CA-TYPE CA-VALUE, The max number of address is 10, the range of CA-TYPE is 0-255, the length of CA-VALUE is [1-232]

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

The following example shows how to configure MED location-id tlv :

```
Switch# configure terminal
Switch(config)# interface eth-0-1
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.16 debug lldp**Command Purpose**

Use this command to turn on the debug switches of LLDP module.
To restore the default, use the no form of this command

Command Syntax

```
debug lldp ( events | packet | all | tlv-info )
no debug lldp ( events | packet | all | tlv-info )
```

Parameter	Parameter Description	Parameter Value
events	LLDP events	-
packet	LLDP Packet information	-
all	Turn all debugging on	-
tlv-info	Enable TLV information debugs	-

Command Mode

Privileged EXEC

Default

None

Usage

Use command "terminal monitor" to make debug messages print on the VTY immediately.
Use command "show logging buffer" to check the debug messages in the logging buffer.

Examples

The following is sample to open lldp debug switches:

```
Switch# debug lldp all
```

Related Commands

terminal monitor
show logging buffer

15.7.17 show lldp local

Command Purpose

To display the LLDP local information, use the show lldp local command in privileged EXEC mode.

Command Syntax

show lldp local (config | tlv-info) (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
config	Configuration Information	-
tlv-info	Local LLDP TLV information	-
interface	Display LLDP configuration or tlv information of special interface	-
IFNAME	Interface name, only allowed physical interface	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

If interface is not specified, this command will display the global information of LLDP.

Examples

The following example shows how to display LLDP configuration:

```
Switch# show lldp local config
```

```
LLDP global configuration:
```

```
=====
LLDP function global enabled : NO
LLDP msgTxHold      : 4
LLDP msgTxInterval : 30
LLDP reinitDelay   : 2
LLDP txDelay       : 2
Switch# show lldp local config interface eth-0-4
LLDP configuration on interface eth-0-4 :
```

```
=====
LLDP admin status : Disabled
```

```
Basic optional TLV Enabled:
```

```
  Port Description TLV
  System Name TLV
  System Description TLV
  System Capabilities TLV
  Management Address TLV
```

```
IEEE 802.1 TLV Enabled:
```

```
  Port Vlan ID TLV
  Port and Protocol Vlan ID TLV
  Vlan Name TLV
  Protocol Identity TLV
```

```
IEEE 802.3 TLV Enabled:
```

```
  MAC/PHY Configuration/Status TLV
  PowerVia MDI TLV
  Link Aggregation TLV
  Maximum Frame Size TLV
```

```
LLDP-MED TLV Enabled:
```

```
  Med Capabilities TLV
  Network Policy TLV
```

Extended Power-via-MDI TLV Inventory TLV

Related Commands

lldp enable(global)
lldp enable(interface)
lldp tlv basic
lldp tlv med
lldp tlv 8023-org-specific
lldp tlv 8021-org-specific
lldp msg-tx-hold
lldp timer msg-tx-interval
lldp timer reinitDelay
lldp timer tx-delay

15.7.18 show lldp neighbor

Command Purpose

To display LLDP neighbor information, use the show lldp neighbor command in privileged EXEC mode.

Command Syntax

show lldp neighbor (interface *IFNAME* |) (brief |)

Parameter	Parameter Description	Parameter Value
interface	Display LLDP neighbor information of special interface	-
IFNAME	Interface name, only allowed physical interface	Support physical ports
brief	Display brief information	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the LLDP neighbor information.

Examples

The following example shows how to display LLDP neighbor information:

Switch# show lldp neighbor interface eth-0/4 brief

```
Local Port   : eth-0/4
Remote Port  : eth-0/6
Hold Time    : 120
Expire Time  : 116
System Name  : switch
-----
```

Related Commands

lldp enable(global)
lldp enable(interface)

15.7.19 show lldp statistics

Command Purpose

To display the statistics of LLDP packets, use the show lldp statistics command in privileged EXEC mode.

Command Syntax

show lldp statistics (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
interface	Display LLDP statistics of special interface	-
IFNAME	Interface name, only allowed physical interface	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display detail LLDP statistics.

Examples

The following example shows how to display LLDP statistics:

```
Switch# show lldp statistics interface eth-0-4
```

LLDP statistics information:

=====

LLDP Port statistics for eth-0-4

Frames transmitted: 568

Frames Aged out: 0

Frames Discarded: 0

Frames with Error: 0

Frames Recieved: 364

TLVs discarded: 0

TLVs unrecognized: 0

Related Commands

clear lldp statistics

15.7.20 clear lldp statistics

Command Purpose

To reset the statistics of LLDP packets , use the clear lldp statistics command in privileged EXEC mode.

Command Syntax

clear lldp statistics (interface *IFNAME* |)

Parameter	Parameter Description	Parameter Value
interface	Clear LLDP statistics of special interface	-
IFNAME	Interface name, only allowed physical interface	Support physical ports

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to reset LLDP statistics.

Examples

The following example shows how to clear LLDP statistics:

```
Switch# clear lldp statistics
```

Related Commands

show lldp statistics

Chapter 16 VPN Commands

16.1 VRF Commands

16.1.1 ip vrf

Command Purpose

To configure a VPN routing and forwarding (VRF) routing table, use the `ip vrf` command in global configuration mode. To remove a VRF routing table, use the `no` form of this command.

Command Syntax

`ip vrf VRF-NAME`

`no ip vrf VRF-NAME`

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Global Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf ComA
Switch(config-vrf)# route-target both 100:2
Switch(config-vrf)# route-target import 200:1
```

Related Commands

`ip vrf forwarding`

16.1.2 show ip vrf

Command Purpose

To show the set of defined VRFs and associated interfaces, use the `show ip vrf` command in Privileged EXEC mode.

Command Syntax

`show ip vrf ( bgp ( brief | detail ) | interfaces | ospf | rip | VRF-NAME | )`

Parameter	Parameter Description	Parameter Value
bgp	Border Gateway Protocol (BGP)	-
brief	Brief VPN Routing/Forwarding instance information	-
detail	Detailed VPN Routing/Forwarding instance information	-
interfaces	Show VPN Routing/Forwarding interface information	-
ospf	Open Shortest Path First (OSPF)	-
rip	Routing Information Protocol (RIP)	-
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# show ip vrf
```

Related Commands

None

16.1.3 ip vrf forwarding

Command Purpose

To associate a VPN routing and forwarding (VRF) instance with an Layer3 interface, use the `ip vrf forwarding` command in interface configuration mode. To disassociate a VRF, use the `no` form of this command.

Command Syntax

ip vrf forwarding *VRF-NAME*

no ip vrf forwarding

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Interface Configuration

Default

None

Usage

Executing this command on an interface removes the IP address on this interface, The IP address should be reconfigured.

Examples

```
Switch# configure terminal
Switch(config)# ip vrf ComA
Switch(config-vrf)# exit
Switch(config)# interface eth-0-1
Switch(config-if)# no switchport
Switch(config-if)# ip vrf forwarding ComA
```

Related Commands

ip vrf

ip route vrf

16.1.4 ip route vrf

Command Purpose

To establish static routes for a VPN routing and forwarding (VRF) instance, use the ip route vrf command in global configuration mode. To remove static routes, use the no form of this command.

Command Syntax

ip route vrf *VRF-NAME DST_NET NH_ADDR*

no ip route vrf *VRF-NAME DST_NET NH_ADDR*

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters
DST_NET	Destination IP subnet, the format can be target IP address with masklen(A.B.C.D/M) or target IP address with netmask (A.B.C.D A.B.C.D)	The format can be target IP address with masklen(A.B.C.D/M) or target IP address with netmask (A.B.C.D A.B.C.D)
NH_ADDR	Next-hop IP address, the format should be A.B.C.D	IPv4 Address

Command Mode

Global Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip route vrf VPN-NAME 2.2.2.0/24 1.1.1.2
```

Related Commands

show ip route vrf

16.1.5 arp vrf

Command Purpose

To add a permanent entry in the Address Resolution Protocol (ARP) cache for VRF, use the arp vrf command in global configuration mode. To remove an entry from VRF ARP cache, enter the no form of this command.

Command Syntax

```
arp vrf VRF_NAME IP_ADDR MAC
no arp vrf VRF_NAME IP_ADDR
```


Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters
IP_ADDR	IP address of the ARP entry	IPv4 Address
MAC	Hardware address of the ARP entry in HHHH.HHHH.HHHH format	MAC Address

Command Mode

Global Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# arp vrf vpn3 1.1.1.1 0000.1111.2222
```

Related Commands

```
show ip arp vrf VRF-NAME
clear ip arp vrf VRF-NAME A.B.C.D
```

16.1.6 show ip arp vrf

Command Purpose

Use this command to show arp entry in VRF instance.

Command Syntax

```
show ip arp vrf VRF-NAME
```

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display all arp entry in the arp table of the VRF.:

```
Switch# show ip arp vrf ComA
```

Protocol	Address	Age (min)	Hardware Addr	Interface
Internet	1.1.1.1	-	0000.1111.2222	

Related Commands

arp vrf

16.1.7 clear ip arp vrf

Command Purpose

Use this command to refresh a specific dynamic ARP entry from ARP cache for the VRF.

Command Syntax

```
clear ip arp vrf VRF-NAME IP_ADDR
```

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters
IP_ADDR	Dynamic learned ARP entry IP address	IPv4 Address

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to refresh a dynamic arp entry in VRF:

```
Switch# clear ip arp vrf ComA 1.1.1.1
```

Related Commands

arp vrf

16.1.8 ping vrf

Command Purpose

Use this command to ping address in VRF.

Command Syntax

ping vrf *VRF-NAME* *IPv4_HOST*

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	-
IPv4_HOST	Ping destination address or hostname	IPv4 Address or host name string

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# ping vrf vpn 1.1.1.1
```

```
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.  
64 bytes from 1.1.1.1: icmp_seq=0 ttl=64 time=0.114 ms  
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=0.087 ms  
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=0.087 ms  
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.097 ms  
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.133 ms  
--- 1.1.1.1 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4041ms  
rtt min/avg/max/mdev = 0.087/0.103/0.133/0.020 ms, pipe 2
```

Related Commands

None

16.1.9 traceroute vrf

Command Purpose

Use this command to trace route in VRF.

Command Syntax

`traceroute vrf VRF-NAME IPV4_HOST`

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters
WORD	Trace route destination address or hostname	IPv4 Address or host name string

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# traceroute vrf vpn 1.1.1.1
```

```
tracert to 1.1.1.1 (1.1.1.1), 30 hops max, 38 byte packets
```

```
1  1.1.1.1 (1.1.1.1)  0.222 ms  0.169 ms  0.169 ms
```

Related Commands

None

16.1.10 telnet vrf

Command Purpose

Use this command to telnet in VRF.

Command Syntax

```
telnet vrf VRF-NAME WORD
```

Parameter	Parameter Description	Parameter Value
VRF-NAME	VPN Routing/Forwarding instance name	Up to 15 characters
WORD	The destination address or hostname for telnet	-

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

```
Switch# telnet vrf vpn 9.9.9.2
```

```
Trying 9.9.9.2...
```

```
Connected to 9.9.9.2.
```

```
Escape character is '^['.
```

```
Fedora Core release 4 (Stentz)
```

```
Kernel 2.6.32.23 on an i686
```

```
login: root
```

```
Password:
```

Related Commands

None

16.1.11 rd

Command Purpose

Use this command to set route distinguisher.

Command Syntax

rd *RD-VALUE*

Parameter	Parameter Description	Parameter Value
RD-VALUE	Route distinguisher value. ASN:nn or IP-address:nn	The range of ASN is 1-4294967295 or in IPv4 format, The range of nn is 1-65535

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# rd 1.1.1.1:1
```

Related Commands

None

16.1.12 route-target

Command Purpose

Use this command to set route target. To unset route target, enter the no form of this command.

Command Syntax

route-target (both | export | import) *RT-VALUE*

no route-target (both | export | import) (*RT-VALUE* |)

Parameter	Parameter Description	Parameter Value
both	Import and export	-
export	Export	-
import	Import	-
RT-VALUE	Route-target value. ASN:nn or IP-address:nn	The range of ASN is 1-4294967295 or in IPv4 format, The range of nn is 1-65535

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# route-target import 100:1
```

Related Commands

None

16.1.13 import map

Command Purpose

Use this command to set import map. To unset import map, enter the no form of this command.

Command Syntax

import map *WORD*

no import map

Parameter	Parameter Description	Parameter Value
WORD	Pointer to route-map entries	Up to 20 characters

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# import map 100
```

Related Commands

export map

16.1.14 export map

Command Purpose

Use this command to set export map.To unset export map, enter the no form of this command.

Command Syntax

export map *WORD*

no export map

Parameter	Parameter Description	Parameter Value
WORD	Pointer to route-map entries	Up to 20 characters

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# export map 100
```

Related Commands

import map

16.1.15 router-id**Command Purpose**

Use this command to set router-id.To unset router-id, enter the no form of this command.

Command Syntax

```
router-id IP_ADDR
no router-id
```

Parameter	Parameter Description	Parameter Value
<i>IP_ADDR</i>	Router identifier in IP address format	IPv4 Address

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# router-id 1.1.1.1
```

Related Commands

show ip vrf

16.1.16 description

Command Purpose

Use this command to specific VRF description.To remove VRF description, enter the no form of this command.

Command Syntax

description *LINE*
no description

Parameter	Parameter Description	Parameter Value
LINE	Characters describing this VRF	The name length should be no more than 40 and the first character must be a-z, A-Z or 0-9.

Command Mode

VRF Configuration

Default

None

Usage

None

Examples

```
Switch# configure terminal
Switch(config)# ip vrf test
Switch(config-vrf)# description VrfName1
```

Related Commands

show ip vrf



 <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.