S3950-4T12S Switch CLI Reference Guide

Model: S3950-4T12S

CLI REFERENCE GUIDE

Content

1 Preface....1
1.1 Declaration....1
1.2 Audience....1
1.3 Conventions....1
2 Basic Commands....2
2.1 System Configuration Commands....2
2.2 User Management Commands....43
2.3 FTP Commands....48
2.4 TFTP Commands....54
2.5 scp Commands....57
2.6 Telnet Commands....60
2.7 SSH Commands....63
2.8 Time&Timezone Commands....80
2.9 License Commands....85
2.10 HTTP commands Commands....86
2.11 RPC-API commands Commands....94
3 Ethernet Commands....97
3.1 Interface Commands....97
3.2 Interface Errdisable Commands....117
3.3 MAC Address Table Commands....126
3.4 VLAN Commands....135
3.5 Voice VLAN Commands....147
3.6 Link Aggregation Commands....151
3.7 VLAN Classification Commands....165
3.8 MSTP Commands....172
3.9 Flow Control Commands....206
3.10 Storm Control Commands....209
3.11 Loopback Detection Commands....211
3.12 MLAG Commands....216
4 IP Service Commands....225
4.1 ARP Commands....225
4.2 DHCP Client Commands....237

4.3 DHCP Relay Commands....248
4.4 DHCP Server Commands....260
4.5 DNS Commands....280
5 IP Routing Commands....285
5.1 IP Unicast-Routing Commands....285
5.2 RIP Commands....295
5.3 Route Map Commands....316
5.4 Prefix-list Commands....341
6 Multicast Commands....347
6.1 IGMP Snooping Commands....347
7 Traffic Management Commands....368
7.1 QOS Commands....368
8 Security Commands....437
8.1 Port Security Commands....437
8.2 Vlan Security Commands....443
8.3 Time Range Commands....447
8.4 ACL Commands....450
8.5 Extend ACL Commands....480
8.6 IEEE 802.1x Commands....508
8.7 Arp Inspection Commands....522
8.8 DHCP Snooping Commands....537
8.9 IP Source Guard Commands....550
8.10 AAA Commands....554
8.11 RADIUS Authentication Commands....563
8.12 Tacacs+Commands....568
8.13 Port Isolate Commands....571
8.14 Private Vlan Commands....573
8.15 DDOS Commands....575
8.16 Key Chain Commands....583
8.17 Port-block Commands....588
8.18 Device management securiy Commands....590
9 Reliability Commands....593
9.1 BHM Commands....593

9.2 CPU Traffic Limit Commands....596
9.3 CPU Traffic Statistics Commands....602
9.4 UDLD Commands....607
9.5 ERPS Commands....612
9.6 Smart-Link Commands....628
9.7 Multi-Link Commands....640
9.8 Monitor Link Commands....655
9.9 VRRP Commands....660
9.10 Track Commands....670
9.11 VARP Commands....687
10 Device Management Commands....689
10.1 STM Commands....689
10.2 Syslog Commands....691
10.3 Mirror Commands....704
10.4 Device Management Commands....720
10.5 Bootrom Commands....725
10.6 Bootup Diagnostic Commands....732
10.7 SmartConfig Commands....734
11 Network Management Commands....736
11.1 Network Diagnosis Commands....736
11.2 NTP Commands....738
11.3 Phy Loopback Commands....753
11.4 RMON Commands....761
11.5 SNMP Commands....769
11.6 SFLOW Commands....792
11.7 LLDP Commands....797
12 VPN Commands....814
12.1 GRE TUNNEL Commands....814

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
Italic type with capital letters	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.

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 200110001 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 exe

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/uImage.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 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

2.1.19 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

2.1.20 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

2.1.21 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

2.1.22 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

2.1.23 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

2.1.24 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	-

Parameter	Parameter Description	Parameter Value
chsm	Chassis management	-
dhclient	DHCP client module	-
dhcpd	DHCP	-
dhcprelay	DHCP relay	-
dhcprelay6	DHCP relay6(IPv6)	-
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

2.1.25 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

None

2.1.26 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?hsrvd
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?lacpd
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?mtdblockd
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

2.1.27 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

2.1.28 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 hsrvd
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

2.1.29 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

2.1.30 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

2.1.31 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

2.1.32 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

2.1.33 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

2.1.34 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)

2.1.35 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

2.1.36 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

2.1.37 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

2.1.38 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

2.1.39 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

2.1.40 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 2011test
drwxrwxrwx 2 4096 Jun 8 2011test1
drwxrwxrwx 2 4096 Jun 7 2011test2
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

2.1.41 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

2.1.42 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

2.1.43 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

2.1.44 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

None

2.1.45 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

2.1.46 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

2.1.47 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

2.1.48 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

2.1.49 show diagnostic-information

Command Purpose

Display diagnstic-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

2.1.50 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

2.1.51 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

2.1.52 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 udisk:

After this operation,you can not use USB disk.
Are you sure to continue?[yes/no]:yes
```

Related Commands

None

2.1.53 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

2.1.54 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

2.1.55 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

None

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

None

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

None

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 ftp:/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

Parameter	Parameter Description	Parameter Value
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

None

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

None

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

None

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

None

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

Related Commands

None

2.6.2 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

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

no 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)#telnet server source address vrf vpn1 10.10.10.1
```

Related Commands

None

2.6.3 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

telnet server source port *NUMBER*

no 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)#telnet server source port 2323
```

Related Commands

None

2.6.4 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

telnet server source mgmt-if port *NUMBER*

no telnet server source mgmt-if port

Parameter	Parameter Description	Parameter Value
mgmt-if port NUMBER	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)#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,modifing 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 NAME	Specify a vrf to provide SSH server	Up to 15 characters
IP_ADDR	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 inbind 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 NUMBER	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)	-

Parameter	Parameter Description	Parameter Value
hmac-sha1-160	SHA1 based HMAC(160 bits,SSHv2 only)	-
hmac-sha1-96	SHA1 based HMAC(96 bits,SSHv2 only)	-
-o numberof-passwordprompts 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	-

Parameter	Parameter Description	Parameter Value
HOUR_OFFSET	Specify the time offset in hours	0-18
MINUTES_OFFSET	[optional]Specify the time offset in minutes,should be in range 0 to 59	0-59
SECCONDS_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.

Parameter	Parameter Description	Parameter Value
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	-
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.	1-120 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 License Commands

2.9.1 generate device identifier

Command Purpose

To generate device identifier,use this command in Privileged EXEC mode.

Command Syntax

generate device identifier(mgmt-if|)*GURLNAME*

generate device identifier(*GFILENAME*|)

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-
GURLNAME	URL name	-
GFILENAME	local file name	-

Command Mode

Privileged EXEC

Default

None

Usage

This command will generate the unique device identifier(UDI)on the current device,customer can get license for the current device form the vendor with UDI.

Examples

The following example shows how to generate UDI:

```
Switch#generate device identifier mgmt-if tftp://10.10.38.160/device.udi
```

Related Commands

None

2.9.2 show license

Command Purpose

To show license on the device,use the show license command in Privileged EXEC mode.

Command Syntax

show license(*GFILENAME*|)

Parameter	Parameter Description	Parameter Value
GFILENAME	local file name	-

Command Mode

Privileged EXEC

Default

None

Usage

This command will show the license on the current device.

Examples

The following example shows how to show license:

```
Switch#show lincese

License files:
=====================================================================
flash:/ma.lic:
Created Time:Fri Dec 6 17:22:23 CST 2013
Vendor:Vendor1
Customer:Customer1
Device MAC:00:1E:08:09:03:00
Feature Set:QINQ MVR ERPS MEF ETHOAM
VPWS VPLS HVPLS SMLK TPOAM
OSPF PIM_SM IGMP VRF MPLS
LDP BGP RSVP OSPF_TE EXTEND_ACL
PTP BFD SSM IPV6 OSPF6
PIM_SM6 MVR6 RIPNG TUNNEL_V6
```

Related Commands

None

2.10 HTTP commands Commands

2.10.1 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

2.10.2 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

2.10.3 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

2.10.4 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

2.10.5 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 NAME	Specify a vrf to provide WEB server	A string with 1-15 characters
A.B.C.D	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

2.10.6 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

2.10.7 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

2.10.8 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
PORT	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

2.10.9 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
PORT	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

2.10.10 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

2.11 RPC-API commands Commands

2.11.1 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
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

2.11.2 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

2.11.3 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

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 or10,000 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*|auto)

no speed

Parameter	Parameter Description	Parameter Value
auto	Port automatically detects the speed it should run	-
10	Port runs at 10 Mb/s	-
100	Port runs at 100 Mb/s	-
1000	Port runs at 1000 Mb/s	-
10G	Port runs at 10Gb/s	-
2G5	Port runs at 2.5Gb/s	-
5G	Port runs at 5Gb/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:

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

Related Commands

None

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 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

3.1.14 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)#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

3.1.15 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 runts,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

3.1.16 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

3.1.17 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

3.1.18 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

3.1.19 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

3.1.20 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)

3.1.21 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

3.1.22 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

3.1.23 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

3.1.24 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	-

Parameter	Parameter Description	Parameter Value
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 fromthe 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

3.1.25 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

3.1.26 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

None

3.1.27 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

3.2 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|udld)

no errdisable detect reason(link-flap|fdb-loop|udld)

Parameter	Parameter Description	Parameter Value
link-flap	Enable detect Link flap error	-
fdb-loop	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 revoery 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 fla p 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

show errdisable detect

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to display the error disable detection reason:

```
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
--------------------------------
bpduguard Disabled
bpduloop 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

None

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.	10-1000000,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 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)vlan VLAN_ID

no MAC_ADDRess-table MAC_ADDR forward(IFNAME|eps EPS_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

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

3.3.3 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_ADDRess-table MAC_ADDR discard

no MAC_ADDRess-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

3.3.4 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
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

3.3.5 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

3.3.6 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	-

Parameter	Parameter Description	Parameter Value
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

3.3.7 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

Parameter	Parameter Description	Parameter Value
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

3.3.8 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

3.3.9 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

3.3.10 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

3.3.11 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:64
Left count:64
Filter address list:
-----------------------------------
```

Related Commands

show mac address-table

3.3.12 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

3.3.13 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 64
```

Related Commands

show resource static-fdb

3.3.14 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#configure terminal
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 swith 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 swith port to trunk mode.

Command Syntax

switchport mode trunk

Command Mode

Interface Configuration

Default

None

Usage

Trunk mode used to connect swith 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 specifid vlan

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 used to allow or forbid the port transmit in specified vlan.

Examples

This example shows how to add the port in vlan11,12:

```
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 vlan11,12:

```
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 transmit in all vlan:

```
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 transmit in all vlan:

```
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#configure terminal
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#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#no vlan 10 bridge disable
```

Related Commands

None

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#configure terminal
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
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	1-55
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	1-55

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 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

3.6.4 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

3.6.5 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

3.6.6 port-channel load-balance

Command Purpose

Use this command to configure the load balance type for the Link Aggregation Control Protocol(LACP).Use the no form of this command to return to the default setting(src-dst-ip).

Command Syntax

port-channel load-balance hash-field-select{ipda|ipsa|macda|macsa|sourceport|destport|ip-protocol|vxlan-vni|nvgre-vsid|inner-ipda|inner-ipsa|inner-ip-protocol|inner-macda|inner-macsa|inner-sourceport|inner-destport|src-interface}

no port-channel load-balance hash-field-select

Parameter	Parameter Description	Parameter Value
dst-mac	Load balance by destination MAC address	-
src-mac	Load balance by source MAC address	-
dst-ip	Load balance by destination IP address	-
src-ip	Load balance by source IP address	-
dst-port	Load balance by destination port	-
src-port	Load balance by source port	-
src-dst-mac	Load balance by source and destination MAC address	-
src-dst-ip	Load balance by source and destination IP address	-
src-dst-port	Load balance by source and destination port	-
src-interface	Load balance by source interface the packet intput	-

Command Mode

Global Configuration

Default

src-dst-ip

Usage

The packet load-balance default by source and destination ip address.

Examples

This example shows how to configure the load balance type for Link Aggregation Control Protocol(LACP):

```
Switch#configure terminal
Switch(config)#port-channel load-balance src-mac
```

Related Commands

None

3.6.7 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(*GROUP_NUMBER*|)summary

Parameter	Parameter Description	Parameter Value
GROUP_NUMBER	Channel group number	1-55

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-field-select:
ipda ipsa
port-channel group-mode:56

Flags:s-suspend T-standby
D-down/admin down B-in Bundle
R-Layer3 S-Layer2
w-wait U-in use

Aggregator Name Protocol Ports
----------------+------------+-------------------------------------------
agg4(SD)Static eth-0-10(D)
```

Related Commands

None

3.6.8 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	1-55

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:55
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

3.6.9 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	1-55

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
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

3.6.10 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	1-55

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:

Actor Actor Actor
Port System ID Port Number Flags
eth-0-9 32768,e0ef.1a32.7e00 0x9 SA

LACP Actor Actor Actor
Port Priority Oper Key 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

3.6.11 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	1-55

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:

LACP port Admin Oper Port Port
```

```
Port Flags Priority Dev ID key Key Number State
eth-0-9 SP 0 0000.0000.0000 0 0 0x0 0x44
```

Related Commands

None

3.6.12 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	1-55

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:

Partner Partner Partner
Port System ID Port Number Flags
eth-0-9 32768,0000.0000.0000 0x0 SP

LACP Partner Partner Partner
Port Priority Oper Key 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

3.6.13 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	1-55

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 LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
eth-0-9 SA indep 32768 1 1 9 0x4d

Partner's information:

Actor LACP port Oper Port Port
Port Flags Priority Dev ID Key Number State
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 LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
eth-0-9 SA indep 32768 1 1 9 0x4d

Partner's information:

Actor LACP port Oper Port Port
Port Flags Priority Dev ID Key Number State
eth-0-9 SP 0 0000.0000.0000 0 0 0x44
```

Related Commands

None

3.6.14 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	1-55

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 46 38 0 0
```

Related Commands

None

3.6.15 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

3.6.16 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	1-55

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

3.6.17 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

3.6.18 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 debuging 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	-

Parameter	Parameter Description	Parameter Value
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

Parameter	Parameter Description	Parameter Value
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	Specifiy ARP protocol	-
ip	Specifiy IP protocol	-
mpls	Specifiy MPLS protocol	-
mpls-mcast	Specifiy MPLS multi cast protocol	-
pppoe	Specifiy PPPOE protocol	-
rarp	Specifiy 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 MSTP Commands

3.8.1 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-stree

3.8.2 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-stree

3.8.3 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-stree

3.8.4 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-stree

3.8.5 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-stree

3.8.6 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

3.8.7 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

3.8.8 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

3.8.9 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

3.8.10 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

3.8.11 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

3.8.12 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

3.8.13 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

3.8.14 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 deafult value:

```
Switch#configure terminal
Switch(config-if)#no spanning-tree path-cost
```

Related Commands

show spanning-tree interface

3.8.15 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

3.8.16 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

3.8.17 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

3.8.18 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

3.8.19 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

3.8.20 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

3.8.21 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

3.8.22 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

3.8.23 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

3.8.24 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

3.8.25 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 threshole 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

3.8.26 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	-
rstp	rapid spanning tree protocol	-
mstp	multiple spanning tree protocol	-

Command Mode

Global Configuration

Default

The default spanning-tree mode is rstp

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

3.8.27 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 defaule 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

3.8.28 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

3.8.29 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

3.8.30 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

3.8.31 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

3.8.32 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

3.8.33 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

3.8.34 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

3.8.35 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

3.8.36 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

3.8.37 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 t
imer 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

3.8.38 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

3.8.39 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

3.8.40 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

3.8.41 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

3.8.42 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

3.8.43 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 t
imer 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

3.8.44 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

3.8.45 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 1,4-100
1 eth-0-1 2
2 eth-0-1 3
```

Related Commands

None

3.8.46 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:Vlans: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:Vlans: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:Vlans: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

3.8.47 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

None

3.9 Flow Control Commands

3.9.1 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

3.9.2 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

3.9.3 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

3.10 Storm Control Commands

3.10.1 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

3.10.2 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

3.10.3 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

3.11 Loopback Detection Commands

3.11.1 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(config-if)#loopback-detect enable
```

Related Commands

show loopback-detect

3.11.2 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

3.11.3 loopback-detect recovery-time

Command Purpose

Using the loopback-detect recovery-time command,you can set the time for interface recovery from abnormal status.

Using the no loopback-detect recovery-time command,you can restore the default time.

By default,the value for recovery time is the packet-interval*3

Command Syntax

loopback-detect recovery-time *TIME*

no loopback-detect recovery-time

Parameter	Parameter Description	Parameter Value
TIME	recovery time in seconds	1-255,unit:second

Command Mode

Interface Configuration

Default

recovery-time is packet-interval*3

Usage

If the interface is shutdown,this command is useless.

Examples

This example shows how to set the value for recoverying time to 10s:

```
Switch#configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#loopback-detect recovery-time 10
```

Related Commands

show loopback-detect

3.11.4 loopback-detect delay-time

Command Purpose

Using the loopback-detect delay-time on interface for set aciton.

Using the no loopback-detect delay-time to set not delay.

Command Syntax

loopback-detect delay-time *TIME*

no loopback-detect delay-time

Parameter	Parameter Description	Parameter Value
TIME	delay time	1-255,unit:second

Command Mode

Interface Configuration

Default

None

Usage

The no loopback-detect delay-time 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 value for delay time set action to 5s:

```
Switch#configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#loopback-detect delay-time 5
```

Related Commands

show loopback-detect

3.11.5 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

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.	-
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

3.11.6 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

3.11.7 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 loopabck 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

3.12 MLAG Commands

3.12.1 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

3.12.2 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

3.12.3 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 apeer 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

3.12.4 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

3.12.5 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

3.12.6 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

3.12.7 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.	1-55

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

3.12.8 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

3.12.9 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 000000000000
mlag_sysid 001e080a6fca
local_syspri 32768
remote_syspri 0
mlag_syspri 32768
peer-link-
peer conf No
reload-delay 300
```

Related Commands

mlag configuration

3.12.10 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

3.12.11 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.	1-55

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

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>	1-2147483 seconds

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 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

4.1.5 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

4.1.6 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

4.1.7 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

4.1.8 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
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
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

4.1.9 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 statistcs:

```
Switch#clear ip arp statistics
```

Related Commands

show ip arp summary

4.1.10 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 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
INTERFACE-NAME	(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

4.1.11 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
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 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,Dyamic:0,Interface:1)
ARP Pkt Received is:0
ARP Pkt Send number is:1
ARP Pkt Dicard number is:0
```

Related Commands

clear ip arp statistics

4.1.12 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

4.1.13 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

4.1.14 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

4.1.15 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

4.1.16 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

4.1.17 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

Examples

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

4.1.18 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 oninterface 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 form 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
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,ohterwise 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 inteface.

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
WORD	WORD:The name of a DHCP pool	1)the length range should be[1,32) 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
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 serverfor 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
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.-_], 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-address1.1.1.1 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 cann't 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
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
all	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

Parameter	Parameter Description	Parameter Value
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

None

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

5 IP Routing Commands

5.1 IP Unicast-Routing Commands

5.1.1 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

5.1.2 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 unreachables

5.1.3 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 unreachables

ip icmp error-interval

5.1.4 ip unreachables

Command Purpose

To enable send the ICMP unreachable messages generated by the switch,use the ip unreachables command in interface configuration mode.To restore the default value,use the no form of this command.

Command Syntax

ip unreachables

no ip unreachables

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 unreachables
```

Related Commands

ip redirects

ip icmp error-interval

5.1.5 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

5.1.6 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)

5.1.7 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
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

5.1.8 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
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

5.1.9 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

5.1.10 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

5.1.11 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

5.1.12 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-file"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

5.1.13 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

5.1.14 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

5.2 RIP Commands

5.2.1 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 orginated 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

5.2.2 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)

5.2.3 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(ACCESSS-LIST-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 imcoming 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)

5.2.4 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 NAME-OF-CHAIN	Enables authentication and specifies the group of keys that are valid	A String of key chain name
string STRING	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

5.2.5 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

5.2.6 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)

5.2.7 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

5.2.8 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	-
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

5.2.9 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

5.2.10 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

5.2.11 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

5.2.12 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

5.2.13 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
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

5.2.14 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

5.2.15 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

5.2.16 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)

5.2.17 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
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

5.2.18 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 WORD	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

5.2.19 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

5.2.20 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 only RIP Version 2 packets,and 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

5.2.21 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
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

5.2.22 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

5.2.23 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

5.2.24 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	-
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

5.2.25 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 debuging rip

RIP debugging status:
RIP packet debugging is on
```

Related Commands

debug rip

5.2.26 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 NAME	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

5.2.27 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

5.3 Route Map Commands

5.3.1 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'	-
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

5.3.2 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

5.3.3 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

5.3.4 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

5.3.5 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 *ACCESSSLISTID*

no match ip address

Parameter	Parameter Description	Parameter Value
ACCESSSLISTID	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

5.3.6 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

5.3.7 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 *ACCESSSLISTID*

no match ip next-hop[*ACCESSSLISTID*]

Parameter	Parameter Description	Parameter Value
ACCESSSLISTID	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

5.3.8 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

5.3.9 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

5.3.10 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

5.3.11 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 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

5.3.12 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

5.3.13 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

5.3.14 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

5.3.15 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

5.3.16 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

5.3.17 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

5.3.18 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
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

5.3.19 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

5.3.20 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

5.3.21 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*

no set ip next-hop

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

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.

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
```

Related Commands

None

5.3.22 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

5.3.23 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	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

5.3.24 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

5.3.25 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.

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

5.3.26 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

5.3.27 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

5.3.28 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
IPADDRESS	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

5.3.29 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.

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

5.3.30 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	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

5.4 Prefix-list Commands

5.4.1 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 prefix10.0.0.0/8:

```
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

5.4.2 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

5.4.3 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

5.4.4 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

5.4.5 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 Multicast Commands

6.1 IGMP Snooping Commands

6.1.1 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

6.1.2 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
VLAN_ID	Vlan ID	1-4094

Command Mode

Global Configuration

Default

Disable

Usage

This command will overide 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

6.1.3 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

6.1.4 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

6.1.5 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

6.1.6 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

6.1.7 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

6.1.8 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

6.1.9 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

6.1.10 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
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)#ip igmp snooping discard-unknown
```

Related Commands

show ip igmp snooping

show ip igmp snooping vlan

6.1.11 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	1-10 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

6.1.12 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

6.1.13 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 specificed 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

6.1.14 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

6.1.15 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
VLAN_ID	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

6.1.16 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

6.1.17 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

6.1.18 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

6.1.19 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

6.1.20 clear ip igmp snooping vlan

Command Purpose

Use this command to clear igmp snooping groups on vlan.

Command Syntax

clear 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

6.1.21 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

6.1.22 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

6.1.23 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

6.1.24 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

6.1.25 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 Respose 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

6.1.26 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

6.1.27 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

6.1.28 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

7 Traffic Management Commands

7.1 QOS Commands

7.1.1 show qos

Command Purpose

Use this command to show whether QoS is enable globally.

Command Syntax

show qos

Command Mode

Priviledge EXEC

Default

None

Usage

This command is used to show QoS configurations globally.

Examples

This example shows how to enable QoS globally:

```
Switch#show qos
Disable
```

Related Commands

qos enable

7.1.2 show qos interface

Command Purpose

Use this command to show QoS configurations for an interface.

Command Syntax

show qos interface *IFNAME*

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Only support physical port and aggregate port

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show QoS configurations for an interface.Configuration is different under different QoS profiles.

Examples

This example shows the QoS queue for enterprise profile:

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

Interface QoS domain:0
Interface trust state:cos
Interface default CoS value:0
Schedule mode:SP(between Class),WDRR(between queue in the same Class)
The number of class on interface:8
Strict priority class ID:7 6 5 4 3 2 1 0
The number of egress queue:8
Queue 0 class 3,DRR weight 1
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 1 class 3,DRR weight 1
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 2 class 4,DRR weight 4
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 3 class 4,DRR weight 10
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 4 class 4,DRR weight 10
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 5 class 4,DRR weight 10
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 6 class 5,DRR weight 1
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue 7 class 7,DRR weight 1
Tail drop mode
Tail drop threshold(Tresh0 Tresh1 Tresh2):224 240 256
Queue shape with CIR 300000 kbps,PIR 300000 kbps
```

Related Commands

qos domain

trust

cos

queue class

queue random-detect

queue tail-drop threshold

queue drr-weight

7.1.3 show qos aggregator-policer

Command Purpose

Use this command to show aggregator-policer information.

Command Syntax

show qos aggregator-policer(*NAME*|)(statistics|)

Parameter	Parameter Description	Parameter Value
NAME	aggregate policer name	-
statistics	Show the statistics of the aggregator policer	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show aggregator-policer information.

Examples

```
Switch#show qos aggregator-policer

AGGREGATOR-POLICER-NAME:agg_plc
mode rfc2697,CIR 4000 kbps,CBS 16000 bytes,EBS 16000 bytes,color blind mode,drop color is red use-l3-length
```

Related Commands

policer-aggregate

aggregate-policer

7.1.4 show policy-map statistics interface

Command Purpose

Use this command to show the statistics of policy-map on interface.

Command Syntax

show policy-map statistics interface *NAME*(input|output)(ace-based|class-based|)(class *CMAP-NAME*|)

Parameter	Parameter Description	Parameter Value
NAME	interface name	Only support physical port and aggregate port
input	The statistics of input direction will be shown	-
output	The statistics of output 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 statistics interface eth-0-1 input ace-based class cmap

Interface:eth-0-1
Ingress service policy:pmap
Class name:cmap,operator:match-any
access-group ipacl
10 permit any any any(1 match 64 bytes)
total 1 match 64 bytes
```

Related Commands

policy-map

show policy-map

show running-config policy-map

7.1.5 show policy-map statistics

Command Purpose

Use this command to show the statistics of policy-map on all interface.

Command Syntax

show policy-map statistics(input|output)(ace-based|class-based|)(class *CMAP-NAME*|)

Parameter	Parameter Description	Parameter Value
input	The statistics of input direction will be shown	-
output	The statistics of output 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 statistics input ace-based

Interface:eth-0-1
Ingress service policy:pmap1
Class name:cmap1,operator:match-any
access-group acl1
10 permit any host 1.1.1.1 2.2.2.0 0.0.0.255 dscp 46(0 match 0 bytes)
20 deny any any any(0 match 0 bytes)
access-group acl2
10 deny src-mac any dest-mac host 0000.1100.0001 vlan 100(0 match 0 bytes)
20 permit src-mac any dest-mac any(0 match 0 bytes)
total 0 match 0 bytes
Class name:class-default,operator:match-any(0 match 0 bytes)
total 0 match 0 bytes
Interface:eth-0-2
Ingress service policy:pmap1
Class name:cmap1,operator:match-any
access-group acl1
10 permit any host 1.1.1.1 2.2.2.0 0.0.0.255 dscp 46(0 match 0 bytes)
20 deny any any any(0 match 0 bytes)
access-group acl2
10 deny src-mac any dest-mac host 0000.1100.0001 vlan 100(0 match 0 bytes)
20 permit src-mac any dest-mac any(0 match 0 bytes)
total 0 match 0 bytes
Class name:class-default,operator:match-any(0 match 0 bytes)
total 0 match 0 bytes
```

Related Commands

policy-map

show policy-map

show running-config policy-map

7.1.6 show qos domain map-table all

Command Purpose

Use this command to display the both ingress and egress information of QoS map-table.

Command Syntax

show qos domain map-table all(default|running)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
default	default configuration	-
running	running configuration	-

Command Mode

Priviledge EXEC

Default

None

Usage

Using this command,the mapping table for qos domain can be shown.

Examples

This example shows how to display the default information of map-table in QoS domain 1:

```
Switch#show qos domain 1 map-table all default

Switch#show qos domain 1 map-table all default

QoS DOMAIN 1,CFI disable,COS map to PRIORITY&COLOR:
-------------------------------------------
COS:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green


QoS DOMAIN 1,DSCP map to PRIORITY&COLOR:
-------------------------------------------
DSCP:0 1 2 3 4 5 6 7
priority:0 1 2 3 4 5 6 7
color:green green green green green green green green
-------------------------------------------
DSCP:8 9 10 11 12 13 14 15
priority:8 9 10 11 12 13 14 15
color:green green green green green green green green
-------------------------------------------
DSCP:16 17 18 19 20 21 22 23
priority:16 17 18 19 20 21 22 23
color:green green green green green green green green
-------------------------------------------
DSCP:24 25 26 27 28 29 30 31
priority:24 25 26 27 28 29 30 31
color:green green green green green green green green
-------------------------------------------
DSCP:32 33 34 35 36 37 38 39
priority:32 33 34 35 36 37 38 39
color:green green green green green green green green
-------------------------------------------
DSCP:40 41 42 43 44 45 46 47
priority:40 41 42 43 44 45 46 47
color:green green green green green green green green
-------------------------------------------
DSCP:48 49 50 51 52 53 54 55
priority:48 49 50 51 52 53 54 55
color:green green green green green green green green
-------------------------------------------
DSCP:56 57 58 59 60 61 62 63
priority:56 57 58 59 60 61 62 63
color:green green green green green green green green
```

```
QoS DOMAIN 1,IP PRECEDENCE map to PRIORITY&COLOR:
---------------------------------------------
IP-prec:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green


QoS DOMAIN 1,EXP map to PRIORITY&COLOR:
---------------------------------------------
EXP:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green





QoS DOMAIN 1,CFI disable,PRIORITY&COLOR map to COS:
|COLOR:
|red yellow green
---------------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
```

```
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 COS value


QoS DOMAIN 1,PRIORITY&COLOR map to DSCP:
|COLOR:
|red yellow green
-------------------------------------------
PRIORITY:0|0 0 0
1|1 1 1
2|2 2 2
3|3 3 3
4|4 4 4
5|5 5 5
6|6 6 6
7|7 7 7
8|8 8 8
9|9 9 9
10|10 10 10
11|11 11 11
12|12 12 12
13|13 13 13
14|14 14 14
15|15 15 15
16|16 16 16
17|17 17 17
18|18 18 18
19|19 19 19
20|20 20 20
21|21 21 21
22|22 22 22
23|23 23 23
24|24 24 24
25|25 25 25
26|26 26 26
27|27 27 27
28|28 28 28
29|29 29 29
30|30 30 30
31|31 31 31
32|32 32 32
33|33 33 33
34|34 34 34
35|35 35 35
36|36 36 36
37|37 37 37
38|38 38 38
39|39 39 39
40|40 40 40
41|41 41 41
42|42 42 42
43|43 43 43
44|44 44 44
45|45 45 45
46|46 46 46
47|47 47 47
48|48 48 48
49|49 49 49
```

```
50|50 50 50
51|51 51 51
52|52 52 52
53|53 53 53
54|54 54 54
55|55 55 55
56|56 56 56
57|57 57 57
58|58 58 58
59|59 59 59
60|60 60 60
61|61 61 61
62|62 62 62
63|63 63 63 DSCP value


QoS DOMAIN 1,PRIORITY&COLOR map to EXP:
|COLOR:
|red yellow green
---------------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
```

```
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 EXP value
```

This example shows how to display the running information of map-table in QoS domain 1:

```
Switch#show qos domain 1 map-table all running

Switch#show qos domain 1 map-table all running

QoS DOMAIN 1,CFI disable,COS map to PRIORITY&COLOR:
---------------------------------------------
COS:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green


QoS DOMAIN 1,DSCP map to PRIORITY&COLOR:
---------------------------------------------
DSCP:0 1 2 3 4 5 6 7
priority:0 1 2 3 4 5 6 7
color:green green green green green green green green
---------------------------------------------
DSCP:8 9 10 11 12 13 14 15
priority:8 9 10 11 12 13 14 15
color:green green green green green green green green
---------------------------------------------
DSCP:16 17 18 19 20 21 22 23
priority:16 17 18 19 20 21 22 23
color:green green green green green green green green
---------------------------------------------
DSCP:24 25 26 27 28 29 30 31
priority:24 25 26 27 28 29 30 31
color:green green green green green green green green
---------------------------------------------
DSCP:32 33 34 35 36 37 38 39
priority:32 33 34 35 36 37 38 39
color:green green green green green green green green
---------------------------------------------
DSCP:40 41 42 43 44 45 46 47
priority:40 41 42 43 44 45 46 47
color:green green green green green green green green
---------------------------------------------
DSCP:48 49 50 51 52 53 54 55
priority:48 49 50 51 52 53 54 55
color:green green green green green green green green
---------------------------------------------
DSCP:56 57 58 59 60 61 62 63
priority:56 57 58 59 60 61 62 63
color:green green green green green green green green


QoS DOMAIN 1,IP PRECEDENCE map to PRIORITY&COLOR:
---------------------------------------------
IP-prec:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green


QoS DOMAIN 1,EXP map to PRIORITY&COLOR:
---------------------------------------------
EXP:0 1 2 3 4 5 6 7
```

```
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green




QoS DOMAIN 1,CFI disable,PRIORITY&COLOR map to COS:
|COLOR:
|red yellow green
-------------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
```

```
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 COS value


QoS DOMAIN 1,PRIORITY&COLOR map to DSCP:
|COLOR:
|red yellow green
-------------------------------------------
PRIORITY:0|0 0 0
1|1 1 1
2|2 2 2
3|3 3 3
4|4 4 4
5|5 5 5
6|6 6 6
7|7 7 7
8|8 8 8
9|9 9 9
10|10 10 10
11|11 11 11
12|12 12 12
13|13 13 13
14|14 14 14
15|15 15 15
16|16 16 16
17|17 17 17
18|18 18 18
19|19 19 19
20|20 20 20
21|21 21 21
22|22 22 22
23|23 23 23
24|24 24 24
25|25 25 25
26|26 26 26
27|27 27 27
28|28 28 28
29|29 29 29
30|30 30 30
31|31 31 31
32|32 32 32
33|33 33 33
34|34 34 34
35|35 35 35
36|36 36 36
37|37 37 37
38|38 38 38
39|39 39 39
40|40 40 40
41|41 41 41
42|42 42 42
43|43 43 43
44|44 44 44
45|45 45 45
46|46 46 46
47|47 47 47
48|48 48 48
49|49 49 49
50|50 50 50
51|51 51 51
52|52 52 52
53|53 53 53
54|54 54 54
55|55 55 55
56|56 56 56
57|57 57 57
58|58 58 58
59|59 59 59
60|60 60 60
61|61 61 61
```

```
62|62 62 62
63|63 63 63 DSCP value


QoS DOMAIN 1,PRIORITY&COLOR map to EXP:
|COLOR:
|red yellow green
---------------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 EXP value
```

Related Commands

show qos domain map-table egress

show qos domain map-table ingress

7.1.7 show qos domain map-table ingress

Command Purpose

Use this command to display the ingress information of qos map-table.

Command Syntax

show qos domain *DOMAIN-NUMBER* map-table ingress(all|cos-priority-color|cos-phb|dscp-priority-color|dscp-phb|exp-priority-color|exp-phb|ip-prec-priority-color|ip-prec-phb)(default|running)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
all	All ingress map table	-
cos-priority-color	cos map to priority and color	-
cos-phb	cos map to PHB	-
dscp-priority-color	dscp map to priority and color	-
dscp-phb	dscp map to PHB	-
exp-priority-color	exp map to priority and color	-
exp-phb	exp map to PHB	-
ip-prec-priority-color	ip precedence map to priority and color	-
ip-prec-phb	ip-prec map to PHB	-
default	default configuration	-
running	running configuration	-

Command Mode

Priviledge EXEC

Default

None

Usage

Using this command,the ingress mapping table for QoS domain can be shown.cos/dscp/exp/ip-prec to priority and color can be shown under basic profile;cos/dscp/exp/ip-prec to PHB can be shown under enterprise profile.

Examples

This example shows how to display the ingress information of qos map-table:

```
Switch#show qos domain 1 map-table ingress all default

Switch#show qos domain 1 map-table ingress all default

QoS DOMAIN 1,CFI disable,COS map to PRIORITY&COLOR:
-----------------------------------------
```

```
COS:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green



QoS DOMAIN 1,DSCP map to PRIORITY&COLOR:
-------------------------------------------
DSCP:0 1 2 3 4 5 6 7
priority:0 1 2 3 4 5 6 7
color:green green green green green green green green
-------------------------------------------
DSCP:8 9 10 11 12 13 14 15
priority:8 9 10 11 12 13 14 15
color:green green green green green green green green
-------------------------------------------
DSCP:16 17 18 19 20 21 22 23
priority:16 17 18 19 20 21 22 23
color:green green green green green green green green
-------------------------------------------
DSCP:24 25 26 27 28 29 30 31
priority:24 25 26 27 28 29 30 31
color:green green green green green green green green
-------------------------------------------
DSCP:32 33 34 35 36 37 38 39
priority:32 33 34 35 36 37 38 39
color:green green green green green green green green
-------------------------------------------
DSCP:40 41 42 43 44 45 46 47
priority:40 41 42 43 44 45 46 47
color:green green green green green green green green
-------------------------------------------
DSCP:48 49 50 51 52 53 54 55
priority:48 49 50 51 52 53 54 55
color:green green green green green green green green
-------------------------------------------
DSCP:56 57 58 59 60 61 62 63
priority:56 57 58 59 60 61 62 63
color:green green green green green green green green



QoS DOMAIN 1,IP PRECEDENCE map to PRIORITY&COLOR:
-------------------------------------------
IP-prec:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green



QoS DOMAIN 1,EXP map to PRIORITY&COLOR:
-------------------------------------------
EXP:0 1 2 3 4 5 6 7
priority:0 8 16 24 32 40 48 56
color:green green green green green green green green
```

Related Commands

show qos domain map-table all

show qos domain map-table egress

7.1.8 show qos domain map-table egress

Command Purpose

Use this command to display the egress information of qos map-table.

Command Syntax

show qos domain *DOMAIN-NUMBER* map-table egress(all|priority-color-cos|priority-color-dscp|priority-color-exp|phb-cos|phb-dscp|phb-exp)(default|running)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain form 0 to 7	0-7
all	All ingress map table	-
priority-color-cos	priority and color map to cos	-
priority-color-dscp	priority and color map to dscp	-
priority-color-exp	priority and color map to exp	-
phb-cos	PHB map to cos	-
phb-dscp	PHB map to dscp	-
phb-exp	PHB map to exp	-
phb-all	PHB map to all	-
default	default configuration	-
running	running configuration	-

Command Mode

Priviledge EXEC

Default

None

Usage

Using this command,the egress mapping table for qos domain can be shown.priority and color to cos/dscp/exp to can be shown under basic profile;PHB to cos/dscp/exp/ip-prec PHB can be shown under enterprise profile.

Examples

This example shows how to display the egress information of qos map-table:

```
Switch#show qos domain 1 map-table egress all default

Switch#show qos domain 1 map-table egress all default


QoS DOMAIN 1,CFI disable,PRIORITY&COLOR map to COS:
|COLOR:
|red yellow green
-----------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
```

```
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 COS value


QoS DOMAIN 1,PRIORITY&COLOR map to DSCP:
|COLOR:
|red yellow green
---------------------------------------------
PRIORITY:0|0 0 0
1|1 1 1
2|2 2 2
3|3 3 3
4|4 4 4
5|5 5 5
6|6 6 6
7|7 7 7
8|8 8 8
9|9 9 9
10|10 10 10
11|11 11 11
12|12 12 12
13|13 13 13
14|14 14 14
```

```
15|15 15 15
16|16 16 16
17|17 17 17
18|18 18 18
19|19 19 19
20|20 20 20
21|21 21 21
22|22 22 22
23|23 23 23
24|24 24 24
25|25 25 25
26|26 26 26
27|27 27 27
28|28 28 28
29|29 29 29
30|30 30 30
31|31 31 31
32|32 32 32
33|33 33 33
34|34 34 34
35|35 35 35
36|36 36 36
37|37 37 37
38|38 38 38
39|39 39 39
40|40 40 40
41|41 41 41
42|42 42 42
43|43 43 43
44|44 44 44
45|45 45 45
46|46 46 46
47|47 47 47
48|48 48 48
49|49 49 49
50|50 50 50
51|51 51 51
52|52 52 52
53|53 53 53
54|54 54 54
55|55 55 55
56|56 56 56
57|57 57 57
58|58 58 58
59|59 59 59
60|60 60 60
61|61 61 61
62|62 62 62
63|63 63 63 DSCP value


QoS DOMAIN 1,PRIORITY&COLOR map to EXP:
|COLOR:
|red yellow green
-------------------------------------------
PRIORITY:0|0 0 0
1|0 0 0
2|0 0 0
3|0 0 0
4|0 0 0
5|0 0 0
6|0 0 0
7|0 0 0
8|1 1 1
9|1 1 1
10|1 1 1
11|1 1 1
12|1 1 1
13|1 1 1
14|1 1 1
15|1 1 1
16|2 2 2
```

```
17|2 2 2
18|2 2 2
19|2 2 2
20|2 2 2
21|2 2 2
22|2 2 2
23|2 2 2
24|3 3 3
25|3 3 3
26|3 3 3
27|3 3 3
28|3 3 3
29|3 3 3
30|3 3 3
31|3 3 3
32|4 4 4
33|4 4 4
34|4 4 4
35|4 4 4
36|4 4 4
37|4 4 4
38|4 4 4
39|4 4 4
40|5 5 5
41|5 5 5
42|5 5 5
43|5 5 5
44|5 5 5
45|5 5 5
46|5 5 5
47|5 5 5
48|6 6 6
49|6 6 6
50|6 6 6
51|6 6 6
52|6 6 6
53|6 6 6
54|6 6 6
55|6 6 6
56|7 7 7
57|7 7 7
58|7 7 7
59|7 7 7
60|7 7 7
61|7 7 7
62|7 7 7
63|7 7 7 EXP value
```

Related Commands

show qos domain map-table all

show qos domain map-table ingress

7.1.9 show qos map-table priority-color-qid-tid

Command Purpose

Use this command to display mapping between priority/color and queueId/thresholdId of qos map-table.

Command Syntax

show qos map-table priority-color-qid-tid

show qos map-table phb-qid-tid

Parameter	Parameter Description	Parameter Value
priority-color-qid-tid	priority and color map to queueId and thresholdId	-
phb-qid-tid	phb map to queueId and thresholdId	-

Command Mode

Priviledge EXEC

Default

None

Usage

Using this command,the priority/color and queue/threshold mapping relation can be shown.

Examples

This example shows how to display the default map for priority and color to queueId and thresholdId:

```
Switch#show qos map-table priority-color-qid-tid

Switch#show qos map-table priority-color-qid-tid

QoS PRIORITY&COLOR map to QueueId and ThresholdId:
|COLOR:
|red yellow green
-----------------------------------------
PRIORITY:0|(0,0)(0,1)(0,2)
1|(0,0)(0,1)(0,2)
2|(0,0)(0,1)(0,2)
3|(0,0)(0,1)(0,2)
4|(0,0)(0,1)(0,2)
5|(0,0)(0,1)(0,2)
6|(0,0)(0,1)(0,2)
7|(0,0)(0,1)(0,2)
8|(1,0)(1,1)(1,2)
9|(1,0)(1,1)(1,2)
10|(1,0)(1,1)(1,2)
11|(1,0)(1,1)(1,2)
12|(1,0)(1,1)(1,2)
13|(1,0)(1,1)(1,2)
14|(1,0)(1,1)(1,2)
15|(1,0)(1,1)(1,2)
16|(2,0)(2,1)(2,2)
17|(2,0)(2,1)(2,2)
18|(2,0)(2,1)(2,2)
19|(2,0)(2,1)(2,2)
20|(2,0)(2,1)(2,2)
21|(2,0)(2,1)(2,2)
22|(2,0)(2,1)(2,2)
23|(2,0)(2,1)(2,2)
24|(3,0)(3,1)(3,2)
25|(3,0)(3,1)(3,2)
26|(3,0)(3,1)(3,2)
27|(3,0)(3,1)(3,2)
28|(3,0)(3,1)(3,2)
29|(3,0)(3,1)(3,2)
30|(3,0)(3,1)(3,2)
31|(3,0)(3,1)(3,2)
32|(4,0)(4,1)(4,2)
33|(4,0)(4,1)(4,2)
34|(4,0)(4,1)(4,2)
35|(4,0)(4,1)(4,2)
```

```
36|(4,0)(4,1)(4,2)
37|(4,0)(4,1)(4,2)
38|(4,0)(4,1)(4,2)
39|(4,0)(4,1)(4,2)
40|(5,0)(5,1)(5,2)
41|(5,0)(5,1)(5,2)
42|(5,0)(5,1)(5,2)
43|(5,0)(5,1)(5,2)
44|(5,0)(5,1)(5,2)
45|(5,0)(5,1)(5,2)
46|(5,0)(5,1)(5,2)
47|(5,0)(5,1)(5,2)
48|(6,0)(6,1)(6,2)
49|(6,0)(6,1)(6,2)
50|(6,0)(6,1)(6,2)
51|(6,0)(6,1)(6,2)
52|(6,0)(6,1)(6,2)
53|(6,0)(6,1)(6,2)
54|(6,0)(6,1)(6,2)
55|(6,0)(6,1)(6,2)
56|(7,0)(7,1)(7,2)
57|(7,0)(7,1)(7,2)
58|(7,0)(7,1)(7,2)
59|(7,0)(7,1)(7,2)
60|(7,0)(7,1)(7,2)
61|(7,0)(7,1)(7,2)
62|(7,0)(7,1)(7,2)
63|(7,0)(7,1)(7,2)(QueueId,ThresholdId)
```

This example shows how to display the default map for phb to queueId and thresholdId:

```
Switch#show qos map-table phb-qid-tid

Switch#show qos map-table phb-qid-tid

QoS PHB map to QueueId/ThresholdId:
PHB Name|QueueId ThresholdId
--------------------------------------------
cs1|0 2
df|1 2
af11|2 2
af12|2 1
af13|2 0
af21|3 2
af22|3 1
af23|3 0
af31|4 2
af32|4 1
af33|4 0
af41|5 2
af42|5 1
af43|5 0
cs2|6 1
cs3|6 0
cs6|6 2
cs7|6 2
cs4|7 2
cs5|7 2
ef|7 2
```

Related Commands

show qos domain map-table all

show qos domain map-table egress

7.1.10 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 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

This command is used to show class-map information.

Examples

```
Switch#show class-map

CLASS-MAP-NAME:class-default(match-any)
CLASS-MAP-NAME:cmap(match-any)
match access-group:macacl
CLASS-MAP-NAME:cmap2(match-all)
```

Related Commands

show running-config class-map

7.1.11 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 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

This command is used to show policy-map information.

Examples

```
Switch#show policy-map plc_map

POLICY-MAP-NAME:plc_map
State:detached
CLASS-MAP-NAME:cmap
match access-group:macacl
mode rfc2698,CIR 1000 kbps,CBS 16000 bytes,PIR 2000 kbps,PBS 16000 bytes,color blind mode,drop color is red
CLASS-MAP-NAME:cmap2
mode rfc2698,CIR 2000 kbps,CBS 16000 bytes,PIR 3000 kbps,PBS 16000 bytes,color blind mode,drop color is red
```

Related Commands

policy-map

show running-config policy-map

7.1.12 qos enable

Command Purpose

Use this command to enable QoS globally.To disable QoS,use the no form of this command.

Command Syntax

qos enable

no qos enable

Command Mode

Global Configuration

Default

Disabled

Usage

Using this command,the qos can be enabled globally.

Examples

This example shows how to enable QoS globally:

```
Switch(config)#qos enable
```

Related Commands

show qos

7.1.13 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(config)#ipg shaping enable
```

This example shows how to disable shaping to calculate IPG bytes:

```
Switch(config)#no ipg shaping enable
```

Related Commands

None

7.1.14 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.

Examples

This example shows how to configure policer to calculate IPG bytes:

```
Switch(config)#ipg policer enable
```

This example shows how to disable policer to calculate IPG bytes:

```
Switch(config)#no ipg policer enable
```

Related Commands

None

7.1.15 policy-map

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 *NAME*

no policy-map *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

None

Usage

The policy-map can be attached to multiple physical ports at both ingress and egress directions.

Examples

Create a policy-map named pm1:

```
Switch(config)#policy-map pm1
Switch(config-pmap)#quit
```

Delete a policy-map named pm1:

```
Switch(config)#no policy-map pm1
Switch(config)#
```

Related Commands

show policy-map

7.1.16 class-map

Command Purpose

Use this command to create a class-map.To remove the class-map,use the no form of this command.

Command Syntax

class-map(match-all|match-any|)*NAME*

no class-map *NAME*

Parameter	Parameter Description	Parameter Value
match-all	Logical-AND all matching statements under this class-map	-
match-any	Logical-OR all matching statements under this class-map	-
NAME	Specify a class-map name,the name of"class-default"is reserved	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

This command is used to define the traffic class template.

Examples

Create a class-map:

```
Switch(config)#no policy-map pm1
```

Remove a class-map:

```
Switch(config)#no class-map cm1

Switch(config)#class-map match-any cm1
```

Related Commands

show class-map

7.1.17 acl-statistics exclude-drop enable

Command Purpose

Use this command to enable the policy-map acl statistics without discard packets.

Command Syntax

acl-statistics exclude-drop enable

no acl-statistics exclude-drop enable

Command Mode

Policy-map Class-map Configuration

Default

None

Usage

None

Examples

```
Switch#configure terminal
Switch(config)#acl-statistics exclude-drop enable
Switch(config)#policy-map pmap
Switch(config-pmap)#class cmap
Switch(config-pmap-c)#statistics enable
```

Related Commands

show policy-map statistics

7.1.18 qos domain map cos-pri-color

Command Purpose

Use this command to modify the COS-to-Priority/Color or COS-to-PHB map.To return to the default value,use the no form of this command.The command of cos-phb is an alias command for cos-pri-color.

Command Syntax

qos domain *DOMAIN-NUMBER* map cos-pri-color cos *COS* to *PRIORIITY COLOR*

qos domain *DOMAIN-NUMBER* map cos-phb cos *COS* to *PHB-TYPE*

no qos domain *DOMAIN-NUMBER* map cos-pri-color(*COS*)

no qos domain *DOMAIN-NUMBER* map cos-phb(*COS*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
COS	Select which CoS will be specified map.	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet,should be green,red or yellow	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

Default mapping table under enterprise profile

Usage

This command is used to define the mapping table of cos to priority/color or PHB.

Examples

This example shows how to modify the cos-to-priority/color map to map cos 7 to outgoing priority value 63,and to set the color value green for a QoS domain:

```
Switch(config)#qos domain 1 map cos-pri-color cos 7 to 63 green
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map cos-pri-color
```

This example shows how to modify the cos-to-phb map to map cos 5 to outgoing phb af11 for a QoS domain:

```
Switch(config)#qos domain 1 map cos-phb cos 5 to af11
```

Related Commands

show qos domain map-table

7.1.19 qos domain cfi enable

Command Purpose

Use this command to enable canonical format indicator drop in the priority/color or PHB to COS map and COS to PHB or priority/color map.To return to the default value,use the no form of this command.

Command Syntax

qos domain *DOMAIN-NUMBER* cfi enable

no qos domain *DOMAIN-NUMBER* cfi enable

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7

Command Mode

Global Configuration

Default

Disabled

Usage

The field named as Canonical Format Indicator(CFI)of VLAN tag is re-defined at IEEE 802.1ad.The new definition is Drop Eligible Indicator(DEI).Using this command,the DEI bit will be considered on color mapping.

Examples

This example shows how to enable Drop Eligible Indicator(DEI)processing in the priority/color or PHB to COS map and COS to PHB or priority/color map:

```
Switch(config)#qos domain 1 cfi enable
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 cfi enable
```

Related Commands

show qos domain map-table

7.1.20 qos domain map ip-prec-pri-color

Command Purpose

Use this command to modify the IP Precedence to Pri/Color for PHB map.To return to the default value,use the no form of this command.The command of ip-prec-phb is an alias command for ip-prec-pri-color.

Command Syntax

qos domain *DOMAIN-NUMBER* map ip-prec-pri-color ip-prec *IP-PREC* to *PRIORIITY COLOR*

qos domain *DOMAIN-NUMBER* map ip-prec-pri-color ip-prec *IP-PREC* to *PHB-TYPE*

no qos domain *DOMAIN-NUMBER* map ip-prec-pri-color(*IP-PREC*)

no qos domain *DOMAIN-NUMBER* map ip-phb(*IP-PREC*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
IP-PREC	Select which IP Precedence will be specified.	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

Default mapping table under basic profile

Usage

This command is used to define the mapping table of IP Precedence to priority/color.

Examples

This example shows how to modify the ip precedence to pri/color map to map ip prec 7 to outgoing priority value 63,and to set the color value green for a QoS domain:

```
Switch(config)#qos domain 1 map ip-prec-pri-color ip-prec 7 to 63 green
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map ip-prec-pri-color
```

This example shows how to modify the ip precedence to phb map to map ip prec 3 to outgoing phb cs3 for a QoS domain:

```
Switch(config)#qos domain 1 map ip-prec-phb ip-prec 7 to cs3
```

Related Commands

show qos domain map-table

7.1.21 qos domain map dscp-pri-color

Command Purpose

Use this command to modify the dscp-priority-color or dscp-phb map for a particular QoS domain.To return to the default value,use the no form of this command.The command of dscp-phb is an alias command for dscp-pri-color.

Command Syntax

qos domain *DOMAIN-NUMBER* map dscp-pri-color *DSCP* to *PRIORIITY COLOR*

qos domain *DOMAIN-NUMBER* map dscp-pri-color *DSCP* to *PHB-TYPE*

no qos domain *DOMAIN-NUMBER* map dscp-pri-color(*DSCP*)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
DSCP	Select which DSCP will be specified map.	0-63
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet,should be green,red or yellow	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

Default mapping table under enterprise profile

Usage

This command is used to define the mapping table of DSCP to priority/color.

Examples

This example shows how to modify dscp-priority-color map to map incoming dscp value 63 to outgoing priority value 63,and to set the color value green for domain 1:

```
Switch(config)#qos domain 1 map dscp-pri-color 63 to 63 green
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map dscp-pri-color
```

This example show how to modify dscp-phb map to map incoming dscp value 63 to outgoing phb ef(same as priority 12,color green)for domain 1:

```
Switch(config)#qos domain 1 map dscp-phb 63 to ef
```

Related Commands

show qos domain map-table

7.1.22 qos domain map exp-pri-color

Command Purpose

Use this command to modify the exp-to-priority/color or exp-to-phb map.To return to the default value,use the no form of this command.The command of exp-phb is an alias command for exp-pri-color.

Command Syntax

qos domain *DOMAIN-NUMBER* map exp-pri-color exp *EXP* to *PRIORIITY COLOR*

qos domain *DOMAIN-NUMBER* map exp-pri-color exp *EXP* to *PHB-TYPE*

no qos domain *DOMAIN-NUMBER* map exp-pri-color(*EXP*|)

no qos domain *DOMAIN-NUMBER* map exp-phb(*EXP*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
EXP	Select which EXP will be specified map	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet,should be green,red or yellow	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

Default mapping table under enterprise profile

Usage

This command is used to define the mapping table of EXP to priority/color.

Examples

This example shows how to modify the exp-to-priority/color map to map exp 7 to outgoing priority value 63,and to set the color value green for a QoS domain:

```
Switch(config)#qos domain 1 map exp-pri-color exp 7 to 63 green
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map exp-pri-color
```

This example shows how to modify the exp-to-phb map to map exp 3 to outgoing phb af22 for a QoS domain:

```
Switch(config)#qos domain 1 map exp-phb exp 7 to af22
```

Related Commands

show qos domain map-table

7.1.23 qos domain map pri-color-cos

Command Purpose

Use this command to modify the priority/color or PHB to CoS map.To return to the default value,use the no form of this command.The command of phb-cos is an alias command for pri-color-cos.

Command Syntax

qos domain *DOMAIN-NUMBER* map pri-color-cos *PRIORIITY COLOR* to *COS*

qos domain *DOMAIN-NUMBER* map phb-cos *PHB-TYPE* to *COS*

no qos domain *DOMAIN-NUMBER* map pri-color-cos(*PRIORIITY COLOR*|)

no qos domain *DOMAIN-NUMBER* map phb-cos(*PHB-TYPE*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
COS	Select which CoS will be specified map.	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

The default mapping table for priority color to cos

Usage

This command is used to define the mapping table of priority/color to CoS.

Examples

This example shows how to modify the priority/color to CoS map to map outgoing priority value 63 to the color value green and cos value 7:

```
Switch(config)#qos domain 1 map pri-color-cos 63 green to 7
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map pri-color-cos
```

This example shows how to modify the PHB to CoS map to map outgoing PHB af33 to cos value 7:

```
Switch(config)#qos domain 0 map phb-cos af33 to 7
```

Related Commands

show qos domain map-table

7.1.24 qos domain map pri-color-dscp

Command Purpose

Use this command to modify the priority/color or PHB to DSCP map.To return to the default value,use the no form of this command.The command of phb-dscp is an alias command for pri-color-dscp.

Command Syntax

qos domain *DOMAIN-NUMBER* map pri-color-dscp *PRIORIITY COLOR* to *DSCP*

qos domain *DOMAIN-NUMBER* map phb-dscp *PHB-TYPE* to *DSCP*

no qos domain *DOMAIN-NUMBER* map pri-color-dscp(*PRIORIITY COLOR*|)

no qos domain *DOMAIN-NUMBER* map phb-dscp(*PHB-TYPE*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
DSCP	Select which DSCP will be specified map.	0-63
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet,should be green,red or yellow	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

The default mapping table for priority color to DSCP.

Usage

This command is used to define the mapping table of priority/color to DSCP.

Examples

This example shows how to modify the priority/color to DSCP map to map priority value 63 and the color value green to dscp 63:

```
Switch(config)#qos domain 1 map pri-color-dscp 63 green to 63
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map pri-color-dscp
```

This example shows how to modify the PHB to DSCP map to map PHB ef to dscp 63:

```
Switch(config)#qos domain 0 map phb-dscp ef to 63
```

Related Commands

show qos domain map-table

7.1.25 qos domain map pri-color-exp

Command Purpose

Use this command to modify the priority/color or PHB to EXP map.To return to the default value,use the no form of this command.The command of phb-exp is an alias command for pri-color-exp.

Command Syntax

qos domain *DOMAIN-NUMBER* map pri-color-exp *PRIORIITY COLOR* to *EXP*

qos domain *DOMAIN-NUMBER* map phb-exp *PHB-TYPE* to *EXP*

no qos domain *DOMAIN-NUMBER* map pri-color-exp(*PRIORIITY COLOR*|)

no qos domain *DOMAIN-NUMBER* map phb-exp(*PHB-TYPE*|)

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
EXP	Select which EXP will be specified map.The range of EXP is from 0 to 7.	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

Global Configuration

Default

The default mapping table for priority color to EXP.

Usage

This command is used to define the mapping table of priority/color to EXP.

Examples

This example shows how to modify the priority/color to EXP map to map priority value 32 and the color value green to exp 4:

```
Switch(config)#qos domain 1 map pri-color-exp 32 green to 4
```

This example shows how to return to the default value:

```
Switch(config)#no qos domain 1 map pri-color-exp
```

This example shows how to modify the PHB to EXP map to map PHB af33 to exp 2:

```
Switch(config)#qos domain 1 map phb-exp af33 to 2
```

Related Commands

show qos domain map-table

7.1.26 qos policer flow-first

Command Purpose

Use this command to configure the order of executing between port-policing and flow-policing.To return to the default policing execution sequence,use the no form of this command.

Command Syntax

qos policer flow-first

no qos policer flow-first

Command Mode

Global Configuration

Default

Disabled

Usage

If both port policer and flow policer are configured for an interface,the default policing execution sequence is to do port policer first and then flow policer.Use this command the change that execution sequence.

Examples

This example shows how to set flow policing first:

```
Switch(config)#qos policer flow-first
```

Related Commands

policer

port-policer

7.1.27 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* mode rfc2697(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(ebs *EBS-SIZE*|)(drop-color *COLOR*|)(use-l3-length|))(stats|)

qos aggregate-policer *NAME* mode rfc2698(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(pir *PIR-RATE*(pbs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

qos aggregate-policer *NAME* mode(rfc4115|bwp)(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(eir *PIR-RATE*(ebs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

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.
mode	Use rfc2697,rfc2698,rfc4115 or bwp mode	-
color-blind	Color blind mode policer	-
color-aware	Color aware mode policer	-
cir CIR-RATE	CIR-Commit Information Rate	0 to 10,000,000 kbps
cbs CBS-SIZE	CBS-Commit Burst Size	0 to 128,000 bytes
eir EIR-RATE	EIR-Excess Information Rate	0 to 10,000,000 kbps
ebs EBS-SIZE	EBS-Excess Burst Size with the range of 0 to 128,000 bytes	0 to 128,000 bytes
pir PIR-RATE	PIR-Peak Information Rate	0 to 10,000,000 kbps
pbs PBS-SIZE	PBS-Peak Burst Size	0 to 128,000 bytes
drop-color COLOR	drop color configuration includes yellow and red	yellow/red
use-l3-length	Use l3 length for policing	-
stats	enable policer statistics	-

Command Mode

Global Configuration

Default

Disabled

Usage

This command is used to create aggregate-policer instance.Color-blind or Color-aware,SRTCM or TRTCM can be configured.

The max number of aggregate policer and flow policer,which is configured in policy-map,is 128 per line-card.

If policer with statistics is configured,and stats are entered when the policer is created,policer statistics is working.

The statistics cannot be modified after the policer is created.

Examples

This example shows how to create an aggregate-policer named agg_plc for SRTCM mode:

```
Switch(config)#qos aggregate-policer agg_plc mode rfc2697 color-aware cir 10000 cbs 128000 ebs 128000 drop-color red
```

Remove aggregate-policer:

```
Switch(config)#no qos aggregate-policer agg_plc
```

Related Commands

show qos aggregator-policer

policer-aggregate

qos statistics policer

7.1.28 qos statistics policer

Command Purpose

Use this command enable the policer statistics.To disable it,use the no form of this command.

Command Syntax

qos statistics policer

no qos statistics policer

Command Mode

Global Configuration

Default

Disabled

Usage

Using this command,the statistics of policer can be enabled.

Examples

This example shows how to enable the policer statistics:

```
Switch(config)#qos statistics policer
```

This example shows how to disable the policer statistics:

```
Switch(config)#no qos statistics policer
```

Related Commands

None

7.1.29 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

This command is used to clear aggregate policing statistics.

Examples

```
Switch#clear qos aggregate-policer plc_agg statistics
```

Related Commands

qos statistics policer

7.1.30 queue stats

Command Purpose

Use this command enable the queue statistics.To disable it,use the no form of this command.

Command Syntax

queue stats enable

no queue stats enable

Command Mode

Interface Configuration

Default

Disabled

Usage

This command is used to enable en-queue statistics on port.

Examples

This example shows how to enable the queue statistics:

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

This example shows how to disable the queue statistics:

```
Switch(config-if)#no queue stats enable
```

Related Commands

clear qos statistics

7.1.31 service-policy

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(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 an interface	-
output	apply policy-map to the outbound of an interface	-

Command Mode

Interface Configuration

Default

None

Usage

Use the service-policy interface configuration command to apply a policy map defined by the policy-map command to the input or output of a particular interface.

The interface can be physical interface,vlan interface,linkagg interface.

Examples

Configure a policy to ingress of a physical interface:

```
Switch(config)#interface eth-0-1
Switch(config-if)#service-policy input plc_map1
```

Remove a policy from ingress of a physical interface:

```
Switch(config-if)#no service-policy input
```

Related Commands

show qos interface

policy-map

7.1.32 cos

Command Purpose

Use this command to configure default cos value for an interface.To cancel this setting,use the no form of this command.

Command Syntax

cos *COS*

no cos

Parameter	Parameter Description	Parameter Value
COS	Select which CoS will be specified for interface.	0-7

Command Mode

Interface Configuration

Default

The default CoS for each interface is 0.

Usage

The port CoS value is used to map the priority and color proprieties that are assigned to all incoming packets,if the port trust state is set to trust port.

Examples

This example shows how to configure default cos value to 5:

```
Switch(config-if)#cos 5
```

This example shows how to cancel this setting:

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

Related Commands

show qos interface

trust port

7.1.33 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(port|cos(ctag-cos|stag-cos|)|dscp-exp|ip-prec)

no trust

Parameter	Parameter Description	Parameter Value
port	Trust port indicates all incoming packets will be assigned with the priority and color according to the port CoS value.	-
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 stagc-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.	-
dscp-exp	Trust DSCP indicates all incoming IP packets will be assigned with the priority and color according to the packet DSCP field,MPLS packets will be assigned with the priority and color according to the packet EXP field,and for other packets,the priority and color of that packet will be mapped the same as trust CoS.	-
ip-prec	Trust ip-prec indicates all incoming packets will be assigned with the priority and color according to the packet IP-Precedence field.If the packet is not an IP packet,the priority and color of that packet will be mapped the same as trust CoS	-

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 indentified 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(config-if)#trust dscp-exp
```

Related Commands

show qos interface

7.1.34 shape average 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

shape average rate *SHAPE-RATE*

no shape

Parameter	Parameter Description	Parameter Value
SHAPE-RATE	Shaping rate	0 to 10,000,000 kbps

Command Mode

Interface Configuration

Default

Disabled

Usage

It is highly recommend that do not configure shape average rate to 0.It is not normally usage of shaping.

If the queue shaping of this port has been applied as two rate,the sum of CIR of each queue should not large than the minimum between port shaping and port bandwidth.If IPG for shaping is disabled,the port bandwidth should be converted by IPG size.By default,the CIR of each queue is infinite.You should configure each queue shaping to confirm this condition.

Examples

This example shows how to configure shaping for a physical port:

```
Switch(config)#interface eth-0-1
Switch(config-if)#shape average rate 60000
```

Remove shape configuration:

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

Related Commands

shape average percent

7.1.35 port-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

port-policer(input|output)mode rfc2697(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(ebs *EBS-SIZE*|)(drop-color *COLOR*|)(use-l3-length|))(stats|)

port-policer(input|output)mode rfc2698(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(pir *PIR-RATE*(pbs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

port-policer(input|output)mode(rfc4115|bwp)(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(eir *EIR-RATE*(ebs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

no port-policer(input|output)

Parameter	Parameter Description	Parameter Value
input	limit the inboud traffic entering the interface	-
output	limit the outboud traffic leaving from the interface	-
mode	use rfc2697, rfc2698, rfc4115 or bwp mode	-
color-blind	Color blind mode policer	-
color-aware	Color aware mode policer	-
cir CIR-RATE	CIR-Commit Information Rate	0 to 10,000,000 kbps
cbs CBS-SIZE	CBS-Commit Burst Size	0 to 128,000 bytes
eir EIR-RATE	EIR-Excess Information Rate	0 to 10,000,000 kbps
ebs EBS-SIZE	EBS-Excess Burst Size with the range of 0 to 128,000 bytes	0 to 128,000 bytes
pir PIR-RATE	PIR-Peak Information Rate	0 to 10,000,000 kbps
pbs PBS-SIZE	PBS-Peak Burst Size	0 to 128,000 bytes
drop-color COLOR	drop color configuration includes yellow and red	yellow/red
use-l3-length	Use l3 length for policing	-

Command Mode

Interface Configuration

Default

Disabled

Usage

This command is used to configure policing on port level.

Examples

Configure a port-policing to ingress of eth-0-1:

```
Switch(config)#interface eth-0-1
Switch(config-if)#port-policer input color-aware cir 200000 cbs 128000 pir 400000 pbs 128000 drop-color red
```

Remove port-policing from ingress of eth-0-1:

```
Switch(config-if)#no port-policer input

Switch(config)#interface eth-0-1
Switch(config-if)#port-policer input mode rfc2698 color-aware cir 200000 cbs 16000 pir 400000 pbs 16000 drop-color red
```

Related Commands

show qos interface

7.1.36 clear qos port-policer statistics

Command Purpose

Use this command to clear port policing statistics.

Command Syntax

clear qos port-policer statistics *IFNAME*(input|output)

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Only support physical port and aggregate port
input	clear inbound port policing statistics	-
output	clear outbound port policing statistics	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear port policing statistics.

Examples

```
Switch#clear qos port-policer statistics eth-0-1 input
```

Related Commands

qos statistics policer

7.1.37 clear qos statistics queue

Command Purpose

Use this command to clear the queue statistics on specified interface.

Command Syntax

clear qos statistics *IFNAME* queue *QUEUE-ID*

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Only support physical port and aggregate port
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).

Command Mode

Privileged EXEC mode

Default

None

Usage

This command is used to clear the statistics on the specified interface.The clear behavior can be control with per-queue level.

Examples

This example shows how to clear queue 0 statistics on interface eth-0-21:

```
Switch#clear qos statistics eth-0-21 queue 0
```

Related Commands

qos statistics queue

7.1.38 queue drr-weight

Command Purpose

Use this command to the WDRR scheduling weight for each queue.To return it to default value,use the no form of this command.

Command Syntax

queue queue-id drr-weight *WEIGHT*

no queue queue-id drr-weight

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
WEIGHT	The value of DRR weight	1-100

Command Mode

Interface Configuration

Default

Default drr value under basic profile.

Usage

In some DRR weight ratio,user should enlarge queue threshold to ensure the DRR weight is precision.The DRR weight is only consider the normal frame size.Jumbo frame size cannot get the precision results.

Examples

This example shows how to configure the WDRR scheduling weight for queue 5:

```
Switch(config-if)#queue 2 drr-weight 20
```

This example shows how to return the queue bandwidth to default value:

```
Switch(config-if)#no queue 2 drr-weight
```

Related Commands

show qos interface

7.1.39 replace cos

Command Purpose

Use this command to replace the cos field in packets on egress.To remove this setting,use the no form of this command.

Command Syntax

replace cos(ctag-cos|stag-cos|)

no replace cos

Parameter	Parameter Description	Parameter Value
cos	Replace cos of the out packet.When the out packet has two cos,only replace outer cos.	-
stag-cos	Replace cos of the out packet.When the out packet has two cos,only replace outer cos.	-
ctag-cos	Replace inner cos of the out packet.When the out packet has two cos,only replace inner cos.When the out packet has one cos,do nothing.	-

Command Mode

Interface Configuration

Default

On trunk port,the default behavior is replace CoS,otherwise is not replace.

Usage

This command is used to replace the cos field in packets on egress,which is generated according to the Priority-Color-CoS map from the internal priority color value.

Examples

This example shows how to replace the cos field in packets on egress:

```
Switch(config-if)#replace cos
```

This example shows how to remove this setting,:

```
Switch(config-if)#no replace cos
```

Related Commands

show qos interface

7.1.40 replace dscp-exp

Command Purpose

Use this command to replace the dscp or exp field in packets on egress.To remove this setting,use the no form of this command.

Command Syntax

replace dscp-exp

no replace dscp-exp

Command Mode

Interface Configuration

Default

Not replace DSCP/EXP on all port.

Usage

This command is used to replace the DSCP field for IP packets on egress,which is generated according to the Priority-Color-DSCP map from the internal priority color value,or replace the exp field for MPLS packets on egress,which is generated according to the Priority-Color-EXP map from the internal priority color value.

Examples

This example shows how to replace the dscp or exp field in packets on egress:

```
Switch(config-if)#replace dscp-exp
```

This example shows how to remove this setting:

```
Switch(config-if)#no replace dscp-exp
```

Related Commands

show qos interface

7.1.41 queue tail-drop threshold

Command Purpose

Use this command to configure the interface queue threshold.To return this setting to default,use the no form of this command.

Command Syntax

queue QUEUE-ID tail-drop threshold THRESHOLD0 THRESHOLD1 THRESHOLD2

no queue *QUEUE-ID* tail-drop threshold

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port.	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
THRESHOLD0	Tail drop threshold0	0-12284
THRESHOLD1	Tail drop threshold1	1-12285 The value should greater than threshold0
THRESHOLD2	Tail drop threshold2	2-12286 The valye should greater than threshold1

Command Mode

Interface Configuration

Default

The default Tail-Drop threshold is 224 240 256 for three drop precedence on GE port and 576 592 608 for three drop precedence on XG port.The threshold value is based on buffer cell.The buffer cell stands for the granularity of the packet stored on the switch.Each buffer cell is up to 256 bytes.One buffer cell cannot store more than 1 packet.Thus,if the packet is larger than 258 bytes,it can be stored via several buffer cells.

Usage

The command is used to configure the tail drop threshold of different colored packets.Tail drop is the default congestion-avoidance technique on every egress queue.With tail drop,packets are queued until the thresholds are exceeded.When smart buffer is enabled,the thresholds take effect after congestion occurs.

Examples

This example shows how to configure interface queue threshold to 160 320 480:

```
Switch(config-if)#queue 1 tail-drop threshold 160 320 480
```

This example shows how to return this setting to default:

```
Switch(config-if)#no queue 1 tail-drop threshold
```

Related Commands

queue random-detect

queue random-detect max-threshold

queue random-detect min-threshold

queue random-detect drop-probability

smart-buffer enable

7.1.42 queue random-detect

Command Purpose

Use this command to enable random detect mode.To disable it,use the no form of this command.

Command Syntax

queue queue-id random-detect

no queue queue-id random-detect

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port.	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).

Command Mode

Interface Configuration

Default

The default drop mode is Tail-Drop mode.

Usage

If the queue length does not reach the min-threshold,the packets will en-queue normally without any discard.If the queue length reaches min-threshold but not exceed max-threshold,the packets will be discarded randomly according to the drop-probability.The dropping ratio is(drop-probability)/65536.If the queue length exceeds max-threshold,all the packets will be discarded.There are some different drop precedence for WRED behavior.When smart buffer is enabled,the thresholds take effect after congestion occurs.

Examples

This example shows how to enable random detect mode:

```
Switch(config-if)#queue 1 random-detect
```

This example shows how to disable random detect mode:

```
Switch(config-if)#no queue 1 random-detect
```

Related Commands

show qos interface

queue random-detect max-threshold

queue random-detect min-threshold

queue random-detect drop-probability

smart-buffer enable

7.1.43 queue random-detect min-threshold

Command Purpose

Use this command to configure random detect mode min-threshold.To remove this setting,use the no form of this command.

Command Syntax

queue QUEUE-ID random-detect min-threshold THRESHOLD0 THRESHOLD1 THRESHOLD2

no queue *QUEUE-ID* random-detect min-threshold

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port.	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
THRESHOLD0	Random-detect min threshold0	0 to 12286.The min threshold0 should less than the max threshold0.
THRESHOLD1	Random-detect min threshold1	0 to 12286.The min threshold1 should less than the max threshold1.
THRESHOLD2	Random-detect min threshold2	0 to 12286.The min threshold2 should less than the max threshold2.

Command Mode

Interface Configuration

Default

The default WRED minimum threshold is 16 24 32 for three drop precedence.The threshold value is based on buffer cell.The buffer cell stands for the granularity of the packet stored on the switch.Each buffer cell is up to 256 bytes.One buffer cell cannot store more than 1 packet.Thus,if the packet is larger than 258 bytes,it can be stored via several buffer cells.

Usage

If the queue length does not reach the min-threshold,the packets will en-queue normally without any discard.If the queue length reaches min-threshold but not exceed max-threshold,the packets will be discarded randomly according to the drop-probability.The dropping ratio is(drop-probability)/65536.If the queue length exceeds max-threshold,all the packets will be discarded.Each threshold is for the different drop precedence for WRED behavior.

Examples

This example shows how to configure queue 1 random detect mode min-threshold to 16,20 and 24:

```
Switch(config-if)#queue 1 random-detect min-threshold 16 20 24
```

This example shows how to return this setting to default:

```
Switch(config-if)#no queue 1 random-detect min-threshold
```

Related Commands

queue random-detect drop-probability

queue random-detect max-threshold

queue random-detect

7.1.44 queue random-detect max-threshold

Command Purpose

Use this command to configure random detect mode max-threshold.To return this setting to default,use the no form of this command.

Command Syntax

queue QUEUE-ID random-detect max-threshold THRESHOLD0 THRESHOLD1 THRESHOLD2

no queue *QUEUE-ID* random-detect max-threshold

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
THRESHOLD0	Random-detect min threshold0	1 to 12287.The min threshold0 should less than the max threshold0.
THRESHOLD1	Random-detect min threshold1	1 to 12287.The min threshold1 should less than the max threshold1.
THRESHOLD2	Random-detect min threshold2	1 to 12287.The min threshold2 should less than the max threshold2.

Command Mode

Interface Configuration

Default

The default WRED maximum threshold is 480 496 512 for three drop precedence.The threshold value is based on buffer cell.The buffer cell stands for the granularity of the packet stored on the switch.Each buffer cell is up to 256 bytes.One buffer cell cannot store more than 1 packet.Thus,if the packet is larger than 258 bytes,it can be stored via several buffer cells.

Usage

If the queue length does not reach the min-threshold,the packets will en-queue normally without any discard.If the queue length reaches min-threshold but not exceed max-threshold,the packets will be discarded randomly according to the drop-probability.The dropping ratio is(drop-probability)/65536.If the queue length exceeds max-threshold,all the packets will be discarded.Each threshold is for the different drop precedence for WRED behavior.

Examples

This example shows how to configure queue 1 random detect mode max-threshold to 90,92 and 94:

```
Switch(config-if)#queue 1 random-detect max-threshold 90 92 94
```

This example shows how to return this setting to default:

```
Switch(config-if)#no queue 1 random-detect max-threshold
```

Related Commands

queue random-detect drop-probability

queue random-detect min-threshold

queue random-detect

7.1.45 queue random-detect drop-probability

Command Purpose

Use this command to configure random detect mode drop probability.To change back to the default configuration,use the no form of this command.

Command Syntax

queue QUEUE-ID random-detect drop-probability PROBABILITY0 PROBABILITY1 PROBABILITY2

no queue *QUEUE-ID* random-detect drop-probability

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
PROBABILITY0	Random-detect threshold0 drop probability	0-65535
PROBABILITY1	Random-detect threshold1 drop probability	0-65535
PROBABILITY2	Random-detect threshold2 drop probability	0-65535

Command Mode

Interface Configuration

Default

The default WRED drop probability is 1024 for all drop precedence.

Usage

If the queue length does not reach the min-threshold,the packets will en-queue normally without any discard.If the queue length reaches min-threshold but not exceed max-threshold,the packets will be discarded randomly according to the drop-probability.The dropping ratio is(drop-probability)/65536.If the queue length exceeds max-threshold,all the packets will be discarded.Each threshold is for the different drop precedence for WRED behavior.

Examples

This example shows how to configure queue 1 random detect mode drop probability to 128,130 and 132:

```
Switch(config-if)#queue 1 random-detect drop-probability 128 130 132
```

This example shows how to return this setting to default:

```
Switch(config-if)#no queue 1 random-detect drop-probability
```

Related Commands

queue random-detect max-threshold

queue random-detect min-threshold

queue random-detect

7.1.46 queue class

Command Purpose

Use this command to map the queue to specified class.To change back to the default configuration,use the no form of this command.

Command Syntax

queue QUEUE-ID class CLASS-ID

no queue *CLASS-ID* class

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).
CLASS-ID	The class level of queue	0-6

Command Mode

Interface Configuration

Default

queue-id	0	1	2	3	4	5	6	7
class-id	0	1	2	3	4	5	6	7

Usage

Every queue belongs to a class.The class range is from 0 to 7.Class 7 is the highest priority.Several queues can be in a same class,or non queue in some class.Packets are scheduled by SP between classes and WDRR between queues in one class.More details can be found in the User Guide.

Examples

This example shows how to map the queue 1 to class 1:

```
Switch(config-if)#queue 1 class 1
```

This example shows how to change back to the default configuration:

```
Switch(config-if)#no queue 1 class
```

Related Commands

show qos interface

7.1.47 queue shape average percent

Command Purpose

Use this command to configure shaping for a queue of a physical port in percentage mode.To remove queue shaping for a physical port,use the no form of this command.

Command Syntax

queue *QUEUE-ID* shape average percent *CIR*

queue *QUEUE-ID* shape average percent *CIR PIR*

no queue *QUEUE-ID* shape

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).

Parameter	Parameter Description	Parameter Value
CIR	Percent value of interface max bandwidth for commit information rate	0-100
PIR	Percent value of interface max bandwidth for peak information rate.If this value is omitted,it will be same as cir.	0-100

Command Mode

Interface Configuration

Default

None

Usage

It is highly recommend that do not configure queue shape average percent to 0.It is not normally usage of shaping.

If the queue shaping of its port has been applied as two rate,the sum of CIR of each queue should not large than the minimum between port shaping and port bandwidth.If IPG for shaping is disabled,the port bandwidth should be converted by IPG size.By default,the CIR of each queue is infinite.You should configure each queue shaping to confirm this condition.

Examples

This example shows how to configure shaping for a queue:

```
Switch(config)#interface eth-0-1
Switch(config-if)#queue 5 shape average percent 15
```

Remove queue shaping:

```
Switch(config-if)#no queue 5 shape
```

Related Commands

queue shape average rate

7.1.48 queue shape average rate

Command Purpose

Use this command to configure shaping for a queue of a physical port in absolute value mode.To remove queue shaping for a physical port,use the no form of this command.

Command Syntax

queue *QUEUE-ID* shape average rate *CIR*

queue *QUEUE-ID* shape average rate *CIR PIR*

no queue *QUEUE-ID* shape

Parameter	Parameter Description	Parameter Value
QUEUE-ID	The id of queue for egress port	The range of queue id is from 0 to 7(basic/enterprise profile),or from 0 to 11(enterprise advance profile).

Parameter	Parameter Description	Parameter Value
CIR	The value for commit information rate	0 to 10,000,000 kbps
PIR	The value for peak information rate.If this value is omitted,it will be same as cir.	0 to 10,000,000 kbps

Command Mode

Interface Configuration

Default

None

Usage

It is highly recommend that do not configure queue shape average rate to 0.It is not normally usage of shaping.

If the queue shaping of its port has been applied as two rate,the sum of CIR of each queue should not large than the minimum between port shaping and port bandwidth.If IPG for shaping is disabled,the port bandwidth should be converted by IPG size.By default,the CIR of each queue is infinite.You should configure each queue shaping to confirm this condition.

Examples

This example shows how to configure shaping for a queue:

```
Switch(config)#interface eth-0-1
Switch(config-if)#queue 5 shape average rate 150000
```

Remove queue shaping:

```
Switch(config-if)#no queue 5 shape
```

Related Commands

queue shape average percent

7.1.49 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	Specify an 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 mode

Default

None

Usage

Use access-list for match criterion in a class-map.

Examples

Configure an access-list match criterion:

```
Switch(config)#class-map match-any cm2
Switch(config-cmap)#match access-group acl1
```

Remove an access-list match criterion:

```
Switch(config-cmap)#no match access-group acl1
```

Related Commands

mac access-list

ip access-list

policy-map

7.1.50 class

Command Purpose

Use this command to define the traffic class in policy-map by referencing a class-map.To remove the traffic class from the policy-map,use the no form of this command.

Command Syntax

class *NAME*

no class *NAME*

Parameter	Parameter Description	Parameter Value
NAME	Specify a class-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

Policy-map mode

Default

None

Usage

A policy-map can include multiple class-maps.

Examples

Add and delete a class in a policy-map:

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#quit
Switch(config-pmap)#no class cm1
```

Related Commands

policy-map

show policy-map

7.1.51 class class-default

Command Purpose

Use this command to create a default traffic class in a policy-map.To remove the default traffic class from a policy-map,use the no form of this command.

Command Syntax

class class-default

no class class-default

Command Mode

Policy-map mode

Default

None

Usage

If a packet does not match any traffic class in the policy-map,then the packet is classified into the default traffic class,and corresponding actions configured for the default class will be performed on that packet.

Examples

Add and delete a default traffic class in a policy-map:

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class class-default
Switch(config-pmap-c)#quit
Switch(config-pmap)#no class class-default
```

Related Commands

policy-map

show policy-map

7.1.52 trust(config-pmap-c mode)

Command Purpose

Use this command to set trust value for the traffic class in a policy-map.To remove the trust state,use the no form of this command.

Command Syntax

trust(dscp-exp|cos(stag-cos|ctag-cos|)|ip-prec|port)

no trust

Parameter	Parameter Description	Parameter Value
dscp-exp	trust dscp or exp value in classified packets	-
cos	trust cos value in classified packets	-
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 stagc-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.	-
ip-prec	trust ip precedence in classified packets	-
port	trust port default cos value in classified packets	-

Command Mode

Config-pmap-c mode

Default

Trust the CoS value in classified packets.

Usage

This command is used to set trust value for the traffic class.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#trust cos
```

Related Commands

show policy-map

7.1.53 set priority color

Command Purpose

Use this command to set priority and color or PHB for traffic class in the policy-map.To remove this setting,use the no form of this command.

Command Syntax

set priority *PRIORIITY* color *COLOR*

set phb *PHB-TYPE*

no set priority color

no set phb

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	0-7
PRIORITY	The internal priority of packet	0-63
COLOR	Color for packet	green,red or yellow
PHB-TYPE	The type of PHB	One of af11,af12,af13,af21,af22,af23,af31, af32,af33,af41,af42,af43,ef,df,cs1,cs2,cs3,cs4,cs5,cs6 and cs7.

Command Mode

config-pmap-c mode

Default

The priority and color is not configured.

Usage

This command is used to set priority and color of traffic matching this class-map.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#set priority 34 color red
Switch(config-pmap-c)#no set priority color
```

Related Commands

show policy-map

7.1.54 set domain

Command Purpose

Use this command to set QoS domain for traffic class in the policy-map.To remove this setting,use the no form of this command.

Command Syntax

set domain DOMAIN-NUMBER

no set domain

Parameter	Parameter Description	Parameter Value
DOMAIN-NUMBER	QoS domain	1-7

Command Mode

config-pmap-c mode

Default

None

Usage

This command is used to set QoS Domain of traffic matching this class-map。

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#set domain 1
Switch(config-pmap-c)#no set domain
```

Related Commands

show policy-map

7.1.55 set dscp/cos

Command Purpose

Use this command to set DSCP/COS for traffic class in the policy-map.To remove this setting,use the no form of this command.

Command Syntax

set dscp *DSCP*

set cos(ctag-cos|stag-cos|)*COS*

no set dscp

no set cos

Parameter	Parameter Description	Parameter Value
DSCP	DSCP value	0-63
COS	COS value	0-7

Command Mode

config-pmap-c mode

Default

None

Usage

This command is used to set DSCP/COS of traffic matching this class-map when packet is transmitted from device。

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#set dscp 1
Switch(config-pmap-c)#no set dscp
```

Related Commands

show policy-map

7.1.56 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 mode rfc2697(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(ebs *EBS-SIZE*|)(drop-color *COLOR*|)(use-l3-length|))(stats|)

policer mode rfc2698(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(pir *PIR-RATE*(pbs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

policer mode(rfc4115|bwp)(color-blind|color-aware|)cir *CIR-RATE*(cbs *CBS-SIZE*|)(eir *PIR-RATE*(ebs *PBS-SIZE*|))(drop-color *COLOR*|)(use-l3-length|))(stats|)

no policer

Parameter	Parameter Description	Parameter Value
color-blind	Color blind mode policer	-
mode	use rfc2697, rfc2698, rfc4115 or bwp mode	-
color-aware	Color aware mode policer	-
cir CIR-RATE	CIR-Commit Information Rate	0 to 10,000,000 kbps
cbs CBS-SIZE	CBS-Commit Burst Size	0 to 128,000 bytes
eir EIR-RATE	EIR-Excess Information Rate	0 to 10,000,000 kbps
ebs EBS-SIZE	EBS-Excess Burst Size with the range of 0 to 128,000 bytes	0 to 128,000 bytes
pir PIR-RATE	PIR-Peak Information Rate	0 to 10,000,000 kbps
pbs PBS-SIZE	PBS-Peak Burst Size	0 to 128,000 bytes
drop-color COLOR	drop color configuration includes yellow and red	yellow/red
use-l3-length	Use l3 length for policing	-
stats	enable policer statistics	-
mode(rfc2697|rfc2698|rfc4115| bwp)		-

Command Mode

config-pmap-c mode

Default

None

Usage

Define a policer for classified traffic.Color-blind or Color-aware,SRTCM or TRTCM can be configured.

The max number of aggregate policer and this flow policer is 128 per line-card.

If qos statistics policer is configured,and stats are entered when the policer is created,policer statistics is working.

The statistics cannot be modified after the policer is created.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#policer color-aware cir 5000000 cbs 128000 ebs 128000 drop-color red
Switch(config-pmap-c)#no policer

Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#policer mode rfc2697 color-aware cir 5000000 cbs 16000 ebs 16000 drop-color red
Switch(config-pmap-c)#no policer
```

Related Commands

show policy-map

qos statistics policer

7.1.57 policer-aggregate

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

policer-aggregate *NAME*

no 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 mode

Default

None

Usage

If an aggregate policer is applied on many interfaces,the aggregate traffic matching this traffic class for these interfaces is limited by the aggregate policer.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#policer-aggregate agg_plc
Switch(config-pmap-c)#no policer
```

Related Commands

aggregate-policer

show policy-map

7.1.58 redirect

Command Purpose

Use this command to redirect classified traffic to a specified interface.Use the no form of this command to cancel the redirection configuration.

Command Syntax

redirect to interface *IFNAME*

no redirect

Parameter	Parameter Description	Parameter Value
IFNAME	Destination interface name.	Only support physical port and aggregate port

Command Mode

config-pmap-c mode

Default

None

Usage

The flow redirection is not effective when the policy-map is applied on output direction.

If a policy-map is applied on input direction of many interfaces,all classified traffic coming into these interfaces will be redirected.

The traffic matching the deny rules in policy-map should not be redirected.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#redirect to interface eth-0-1
Switch(config-pmap-c)#no redirect
```

Related Commands

show policy-map

7.1.59 flow mirror

Command Purpose

Use this command to set mirror source session.Use the no form of this command to cancel the mirror configuration.

Command Syntax

monitor to session *SESSION-ID*

no monitor

Parameter	Parameter Description	Parameter Value
SESSION-ID	Monitor session number with the range of 1 to 3.	1-3

Command Mode

config-pmap-c mode

Default

None

Usage

If a policy-map is applied on input,output or both direction of many interfaces,all classified traffic coming into,leaving from or both these interface will be monitored.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#monitor to session 1
Switch(config)#monitor session 1 destination interface eth-0-1
Switch(config-pmap-c)#no mirror
```

Related Commands

show policy-map

7.1.60 statistics enable

Command Purpose

Use this command to enable statistics for each ace in class map.Use the no form of this command to disable statistics.

Command Syntax

statistics enable

no statistics enable

Command Mode

config-pmap-c mode

Default

Disabled

Usage

If the class-map operator is match-all,only total statistics of the class-map can be shown.

If it is fail to enable the statistics function,some warning message will be given.

Examples

```
Switch(config)#policy-map pm1
Switch(config-pmap)#class cm1
Switch(config-pmap-c)#statistics enable
Switch(config-pmap-c)#no statistics enable
```

Related Commands

show policy-map statistics interface

clear qos policy-map statistics interface

7.1.61 smart-buffer enable

Command Purpose

Use this command to enable smart buffer globally.Use the no form of this command to disable smart buffer globally.

Command Syntax

smart-buffer enable

no smart-buffer enable

Command Mode

Global Configuration

Default

Enabled

Usage

If the smart buffer is enabled,the queue will adjust its queue threshold automatically according to the resource useage.

Examples

```
Switch(config)#smart-buffer enable
```

Related Commands

None

7.1.62 clear qos policy-map statistics interface

Command Purpose

Use this command to clear flow policing and ace matching statistics.

Command Syntax

clear qos policy-map *NAME* statistics interface(*IFNAME*|)(policer-stats|ace-stats|)

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.

Parameter	Parameter Description	Parameter Value
IFNAME	interface name	Only support physical port and aggregate port
policer-stats	Clear the statistics of policer in policy-map	-

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to clear flow policing and ace matching statistics.

Examples

```
Switch#clear qos policy-map plcy statistics interface eth-0-1 input
```

Related Commands

qos statistics policer

statistics enable

7.1.63 show running-config policy-map

Command Purpose

Use this command to show running-config policy-map information.

Command Syntax

show running-config policy-map

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show running-config for policy-map information.

Examples

```
Switch#show running-config policy-map

class class-default
set phb ef
set domain 1
set dscp 1
set cos 1
policer-aggregate a
```

Related Commands

policy-map

show policy-map

7.1.64 show running-config class-map

Command Purpose

Use this command to show running-config class-map information.

Command Syntax

show running-config class-map

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show running-config for class-map information.

Examples

```
Switch#show running-config class-map

class-map match-any cmap
match access-group macacl
!
class-map match-all cmap2
```

Related Commands

show class-map

7.1.65 qos profile

Command Purpose

Use this command to switch QoS profile.

Command Syntax

qos profile(basic|enterprise)

no qos profile

Parameter	Parameter Description	Parameter Value
basic	In basic profile,the system use priority and color to identify the QoS service level	-
enterprise	In enterprise and enterprise advance profile,the system use php to identify the QoS service level.	-

Command Mode

Global Configuration

Default

Basic profile

Usage

Use this command to switch QoS profile between basic,enterprise and enterprise advance.And only after switch reboots does profile take active.

Examples

This example shows how to switch QoS profile to enterprise:

```
Switch(config)#qos profile enterprise

%Changes to QoS profile have been stored,but cannot take effect until the next reload.
Use'show qos profile'to see what QoS profile is current active.
```

Related Commands

show qos profile

7.1.66 show qos profile

Command Purpose

Use this command to display what QoS profile is current active.

Command Syntax

show qos profile

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show what QoS profile is current active.

Examples

```
Switch#show qos profile

Current queue map is:enterprise
The number of egress queue is:8
QoS PHB map to QueueId/ThresholdId:
PHB Name|QueueId ThresholdId
-----------------------------------------
cs1|0 2
df|1 2
af11|2 2
af12|2 1
af13|2 0
af21|3 2
af22|3 1
af23|3 0
af31|4 2
```

```
af32|4 1
af33|4 0
af41|5 2
af42|5 1
af43|5 0
cs2|6 1
cs3|6 0
```

Related Commands

qos profile

8 Security Commands

8.1 Port Security Commands

8.1.1 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

8.1.2 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

8.1.3 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

8.1.4 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

8.1.5 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

8.1.6 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

8.1.7 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

8.1.8 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

8.1.9 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

8.2 Vlan Security Commands

8.2.1 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 *MAXINUM*

no vlan *VLAN_ID* mac-limit maximum

Parameter	Parameter Description	Parameter Value
VLAN_ID	VLAN id	1-4094
MAXINUM	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

8.2.2 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	-

Parameter	Parameter Description	Parameter Value
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

8.2.3 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

8.2.4 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

8.3 Time Range Commands

8.3.1 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

8.3.2 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

Parameter	Parameter Description	Parameter Value
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

8.3.3 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

8.3.4 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

8.4 ACL Commands

8.4.1 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

8.4.2 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

8.4.3 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
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

8.4.4 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	-

Parameter	Parameter Description	Parameter Value
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

8.4.5 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

8.4.6 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
ACL_NAME	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

8.4.7 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
ACL_NAME	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

8.4.8 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	-
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

8.4.9 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

Parameter	Parameter Description	Parameter Value
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 filer 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

8.4.10 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

8.4.11 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

Parameter	Parameter Description	Parameter Value
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

8.4.12 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

Parameter	Parameter Description	Parameter Value
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 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

8.4.13 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
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

Parameter	Parameter Description	Parameter Value
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

8.4.14 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	0-0xFFFFFF
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

Parameter	Parameter Description	Parameter Value
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	-
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 0xffffff
```

Related Commands

no sequence-num

8.4.15 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	-
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

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 0xffffff
```

Related Commands

no sequence-num

8.4.16 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

Parameter	Parameter Description	Parameter Value
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

8.4.17 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 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

Parameter	Parameter Description	Parameter Value
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
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

8.4.18 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
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	-

Parameter	Parameter Description	Parameter Value
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

8.4.19 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
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

8.4.20 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	-

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 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 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

8.4.21 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	0-0xFFFFFF
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 0xffffff
```

Related Commands

no sequence-num

8.4.22 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

8.5 Extend ACL Commands

8.5.1 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
ACL_NAME	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

8.5.2 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
SEQUENCE_NUM	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

8.5.3 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	-
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

8.5.4 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	-

Parameter	Parameter Description	Parameter Value
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

8.5.5 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	Protocol 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-acll)#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-acll)#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-acll)#3 deny any any any routed-packet
```

Related Commands

no sequence-num

8.5.6 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

Parameter	Parameter Description	Parameter Value
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,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 filer 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

8.5.7 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

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

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

8.5.8 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	-
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

Parameter	Parameter Description	Parameter Value
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-acll)#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-acll)#2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

8.5.9 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	-

Parameter	Parameter Description	Parameter Value
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-acll)#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-acll)#2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

8.5.10 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	-
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

Parameter	Parameter Description	Parameter Value
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-acll)#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-acll)#2 deny igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

8.5.11 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	0-0xFFFFFF
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	-

Parameter	Parameter Description	Parameter Value
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

8.5.12 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	-
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 0xffffff
```

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 any routed-packet
```

Related Commands

no sequence-num

8.5.13 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

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
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	-
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-acll)#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-acll)#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-acll)#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-acll)#4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

8.5.14 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
any	Any source host	-
host SRC_IP	The source IP address of a host	IPv4 Address

Parameter	Parameter Description	Parameter Value
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-acll)#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-acll)#2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

8.5.15 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	-

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

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-acll)#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-acll)#2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

None

8.5.16 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

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
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 permit any IGMP packets:

```
Switch#configure terminal
Switch(config)#ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acll)#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-acll)#2 permit igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

8.5.17 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
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

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

8.5.18 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、	0-0xFFFFFF

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 0xffffff
```

Related Commands

no sequence-num

8.5.19 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-acll)#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-acll)#no remark
```

Related Commands

None

8.5.20 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

8.6 IEEE 802.1x Commands

8.6.1 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

8.6.2 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

8.6.3 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

8.6.4 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

8.6.5 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

8.6.6 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
SECONDS	The time interval(in 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

8.6.7 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

8.6.8 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

8.6.9 dot1x timeout

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.

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

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

8.6.10 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

8.6.11 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

8.6.12 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

8.6.13 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

8.6.14 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

8.6.15 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

8.6.16 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

8.6.17 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

8.7 Arp Inspection Commands

8.7.1 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 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

8.7.2 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

8.7.3 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

8.7.4 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 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

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

8.7.5 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 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

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

8.7.6 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

8.7.7 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

8.7.8 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

8.7.9 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

8.7.10 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

8.7.11 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

8.7.12 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

8.7.13 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

Parameter	Parameter Description	Parameter Value
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

8.7.14 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 loged.

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

8.7.15 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

8.7.16 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

8.7.17 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

8.7.18 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
ACL_NAME	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

8.7.19 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

Parameter	Parameter Description	Parameter Value
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

8.7.20 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

8.7.21 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
ACL_NAME	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

8.8 DHCP Snooping Commands

8.8.1 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

8.8.2 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

8.8.3 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

8.8.4 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

8.8.5 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

8.8.6 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

8.8.7 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

8.8.8 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

8.8.9 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

8.8.10 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

8.8.11 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
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

8.8.12 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

8.8.13 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

8.8.14 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

Parameter	Parameter Description	Parameter Value
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

8.8.15 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

8.8.16 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

8.8.17 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

8.9 IP Source Guard Commands

8.9.1 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

8.9.2 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

8.9.3 ip source maximal binding

Command Purpose

To specify the maximum number of bindings for each interface,use the ip source maximal binding command in global configuration mode.To restore to the default value,use the no form of this command.

Command Syntax

ip source maximal binding number per-port *NUMBER*

no ip source maximal binding number per-port

Parameter	Parameter Description	Parameter Value
NUMBER	Specify maximum number of bindings	0-30

Command Mode

Global Configuration

Default

10

Usage

Using for configuring maximal binding number,and default value is 10.The number 0 indicates no limiation

Examples

The following example shows how to restore the default maximum number of bindings:

```
Switch#configure terminal
Switch(config)#no ip source binding entries
```

The following example shows how to specify the maximum number of bindings:

```
Switch#configure terminal
Switch(config)#ip source maximal binding number per-port 20
```

Related Commands

show ip source binding

8.9.4 ip verify source

Command Purpose

Use the ip verify source interface configuration command on the switch stack or on a standalone switch to enable IP source guard on an interface.Use the no form of this command to disable IP source guard.

Command Syntax

ip verify source(ip|ip-mac|ip-vlan|ip-mac-vlan)

no ip verify source

Parameter	Parameter Description	Parameter Value
ip	Check only IP address	-
ip-mac	Check IP address and MAC address	-
ip-vlan	Check IP address and VLAN	-
ip-mac-vlan	Check IP address,MAC address,and VLAN	-

Command Mode

Interface Configuration

Default

None

Usage

When IP source guard is enabled on an access port,the ip-mac-vlan keyword is equivalent to the ip-mac keyword.

By default,IP source guard is disabled on interfaces.

Examples

The following example shows how to enable IP source guard on an interface:

```
Switch#configure terminal
Switch(config)#interface eth-0-1
Switch(config-if)#ip verify source ip-mac
```

Related Commands

ip source binding

show ip source binding

8.9.5 show ip source binding

Command Purpose

Use the show ip source binding privileged EXEC command to display the IP source bindings on the switch.

Command Syntax

show ip source binding(interface *IFNAME*|)

Parameter	Parameter Description	Parameter Value
IFNAME	Display IP source bindings for a specified interface	-

Command Mode

Privileged EXEC

Default

None

Usage

If interface is not specified,all ip-source-binding entries should be shown.

Examples

The following is sample output from the show ip source binding command:

```
Switch#show ip source binding

The total number of ip binding is 1,the max ip number limit is 127
The total number of ipv6 binding is 0,the max ipv6 number limit is 128
IP source guard binding table:
VLAN MAC Address Type Interface State IP Address
==============================================================================
3 0001.0002.0003 static eth-0-1 ip 10.0.0.2
```

Related Commands

ip source binding

no ip source binding

8.10 AAA Commands

8.10.1 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

8.10.2 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

8.10.3 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

8.10.4 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 logining 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

8.10.5 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

8.10.6 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

8.10.7 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

8.10.8 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

8.10.9 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

8.10.10 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

8.10.11 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

8.10.12 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

8.10.13 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

8.11 RADIUS Authentication Commands

8.11.1 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

8.11.2 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(mgmt-if|)(*IPV4_ADDR*|*IPV6_ADDR*) （auth-port *AUTH_PORT*|）（timeout *SECONDS*|）（retransmit *RETRIES*|）（key *STRING*|）(source-interface *IFNAME*|source-ip *SRC_IP_ADDR*|)

no radius-server host(*IPV4_ADDR*|*IPV6_ADDR*)（auth-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	IPv6 Address
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

Parameter	Parameter Description	Parameter Value
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

8.11.3 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

8.11.4 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

8.11.5 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

8.11.6 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

8.12 Tacacs+Commands

8.12.1 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 *A.B.C.D*({key(8|secret|)*STRING*|timeout *SECONDS*|port *PORT*|single-connection}|)

no tacacs-server host(mgmt-if|)*IP_ADDR*

Parameter	Parameter Description	Parameter Value
mgmt-if	Management port	-

Parameter	Parameter Description	Parameter Value
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

8.12.2 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

8.12.3 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

8.13 Port Isolate Commands

8.13.1 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

8.13.2 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	-
l2	Isolate bridged packets	-

Command Mode

Global Configuration

Default

None

Usage

If configure"port-isolate mode l2",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"l2"

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

8.13.3 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

8.14 Private Vlan Commands

8.14.1 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

8.14.2 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

8.14.3 show private-vlan

Command Purpose

To display the private-vlan configure,use the show private-vlan command in privileged Privileged EXEC.

Command Syntax

show 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

None

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 isloate 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 isloate 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

8.15 DDOS Commands

8.15.1 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

8.15.2 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 sumrf 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

8.15.3 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

8.15.4 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

8.15.5 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

8.15.6 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

8.15.7 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

8.15.8 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

8.15.9 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

8.15.10 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:17307
Resist ICMP Flood packets number:0
Resist SYN Flood packets number:0
Resist Fraggle Attack packets number:0
Resist UDP Flood packets number:0

Current DDoS Prevent mgmt-if statistics:
============================================================
Resist ICMP Flood 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

8.15.11 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 SYN Flood packets number:0
Resist Fraggle Attack packets number:0
Resist UDP Flood packets number:0

Current DDoS Prevent mgmt-if statistics:
============================================================
Resist ICMP Flood 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

8.16 Key Chain Commands

8.16.1 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

8.16.2 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

8.16.3 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

8.16.4 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

8.16.5 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

8.16.6 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
WORD	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

8.17 Port-block Commands

8.17.1 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|)

8.17.2 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)

8.18 Device management securiy Commands

8.18.1 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 enabe 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

8.18.2 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 enabe 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

8.18.3 service password-encryption

Command Purpose

To encrypt password of users and line vtys,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 vtys,after this command is configured,existed password or new configued 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

9 Reliability Commands

9.1 BHM Commands

9.1.1 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

9.1.2 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

9.1.3 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

9.1.4 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	-

Parameter	Parameter Description	Parameter Value
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

9.1.5 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

9.2 CPU Traffic Limit Commands

9.2.1 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

9.2.2 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|sflow-egress|fwd-to-cpu|udld|bfd-learning|bgp|dot1x-mac-bypass|egress-ttl-fail|icmpv6|l2protocol-tunnel|loopback-detection|mirror-to-cpu|ndp|tunnel-gre-keepalive}rate *RATE_RANGE*

no 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|sflow-egress|fwd-to-cpu|udld|bfd-learning|bgp|dot1x-mac-bypass|egress-ttl-fail|icmpv6|l2protocol-tunnel|loopback-detection|mirror-to-cpu|ndp|tunnel-gre-keepalive}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	-
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	-

Parameter	Parameter Description	Parameter Value
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	-
udld	Reason for packets unidirectional link detection protocol	-
bfd-learning	Reason for bfd learning packets	-
dot1x-mac-bypass	Reason for mac auth bypass packets	-
egress-ttl-fail	Reason for egress ttl fail packet	-
icmpv6	Reason for ICMPv6 packet	-
l2protocol-tunnel	Reason for layer2 protocol tunnel packet	-
loopback-detection	Reason for loopback detection packet	-
mirror-to-cpu	Reason for mirror-to-cpu packet	-
ndp	Reason for neighbor discovery protocol packet	-
tunnel-gre-keepalive	Reason for tunnel gre keepalive reply packet	-
RATE_RANGE	Individual rate of streams destined to cpu carried with the reason in kbps	0-1000000

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
arp	640	udld	128

Reason	Rate(pps)	Reason	Rate(pps)
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

9.2.3 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|ip-mtu-fail|ip-option|ucast-ttl-fail|mpls-ttl-fail|igmp|sflow-ingress|sflow-egress|fwd-to-cpu|udld|bfd-learning|bgp|dot1x-mac-bypass|egress-ttl-fail|icmpv6|l2protocol-tunnel|loopback-detection|mirror-to-cpu|ndp|tunnel-gre-keepalive}class *CLASS_RANGE*

no 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|sflow-egress|fwd-to-cpu|udld|bfd-learning|bgp|dot1x-mac-bypass|egress-ttl-fail|icmpv6|l2protocol-tunnel|loopback-detection|mirror-to-cpu|ndp|tunnel-gre-keepalive}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

9.2.4 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 256 1
eapol 128 0
erps 128 3
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
ndp 64 2
icmpv6 64 2
ssh 64 3
telnet 64 3
mlag 1000 1
tcp 64 2
ipda 1000 0
icmp-redirect 128 0
mcast-rpf-fail 128 1
macsa-mismatch 128 0
port-security-discard 128 0
vlan-security-discard 128 0
egress-ttl-fail 64 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 1000 0
mirror-to-cpu 1000 0
Total rate:2048(pps)
```

Related Commands

cpu-traffic-limit total rate

cpu-traffic-limit reason rate

9.3 CPU Traffic Statistics Commands

9.3.1 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

9.3.2 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

9.3.3 show cpu traffic-statistics receive

Command Purpose

Use this command to show CPU receive packets by reason.

Command Syntax

show cpu traffic-statistics receive(bpdu|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
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	-
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	-
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	-
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

9.3.4 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

9.3.5 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

9.4 UDLD Commands

9.4.1 udld enable

Command Purpose

Use this command enable/disable global UDLD state.

Command Syntax

udld enable

no udld enable

Command Mode

Global Configuration

Default

Disabled

Usage

None

Examples

This example shows how to enable global UDLD state:

```
Switch#configure terminal
Switch(config)#udld enable
```

Related Commands

show udld

9.4.2 udld port

Command Purpose

Use this command to enable/disable UDLD state on a specific interface.

Command Syntax

udld port(aggressive|)

no udld 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)#udld port
```

Related Commands

show udld

9.4.3 udld 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

udld message interval *INTERVAL*

no udld 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

9.4.4 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

9.4.5 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

9.4.6 show udld neighbors

Command Purpose

Use this command to show information of UDLD neighbors.

Command Syntax

show udld neighbors

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show UDLD neighbor information:

```
Switch#show udld neighbor

Port Device Name Device ID Port ID Neighbor State
-----------------------------------------------
eth-0-9 DUT2 d4f2.489f.d100 eth-0-9 bidirectional
```

Related Commands

None

9.4.7 debug udld

Command Purpose

Use this command to debug UDLD.

Command Syntax

debug udld(all|packet|events)

no debug udld(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 UDLD debug for packets:

```
Switch#debug udld packet
```

Related Commands

None

9.4.8 show debugging udld

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

9.5 ERPS Commands

9.5.1 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 the use first when config 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

9.5.2 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

9.5.3 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

9.5.4 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 seconde),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

9.5.5 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

9.5.6 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

Parameter	Parameter Description	Parameter Value
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

9.5.7 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)

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	-

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 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

9.5.8 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

9.5.9 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

9.5.10 erps ring interface

Command Purpose

Use this command to set interface for specific ERPS ring instance.

Use no form of this command to unset 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 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

9.5.11 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

Parameter	Parameter Description	Parameter Value
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

9.5.12 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
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

9.5.13 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

Command Mode

Global Configuration

Default

None

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	-

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

9.5.14 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
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

9.5.15 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

9.5.16 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

9.5.17 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

9.5.18 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

9.5.19 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

9.5.20 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

9.5.21 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

9.5.22 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 DOMAINID	ERPS domain ID	1-255
ring RINGID	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

9.5.23 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

9.6 Smart-Link Commands

9.6.1 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

9.6.2 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

9.6.3 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	-
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

9.6.4 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

9.6.5 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

9.6.6 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

9.6.7 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

9.6.8 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

9.6.9 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

9.6.10 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

9.6.11 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

9.6.12 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

9.6.13 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

9.6.14 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

9.6.15 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

9.6.16 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

9.6.17 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

9.7 Multi-Link Commands

9.7.1 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
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

9.7.2 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

9.7.3 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-multilk-group)#interface eth-0-9 master
Switch(config-multilk-group)#interface eth-0-13 slave
Switch(config-multilk-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

9.7.4 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-multilk-group)#protected mstp instance 0
Switch(config-multilk-group)#protected mstp instance 10
Switch(config-multilk-group)#protected mstp instance 100
Switch(config-multilk-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

9.7.5 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-multilk-group)#load-balance instance 10 priority 2
```

Related Commands

show multi-link group

9.7.6 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-multilk-group)#restore time 30
```

Related Commands

show multi-link group

9.7.7 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-multilk-group)#restore enable
```

Related Commands

show multi-link group

9.7.8 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-multilk-group)#flush send control-vlan 4 password simple test
```

Related Commands

show multi-link group

multi-link flush receive

9.7.9 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-multilk-group)#group enable
```

Related Commands

show multi-link group

9.7.10 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

9.7.11 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

9.7.12 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

9.7.13 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

9.7.14 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 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

None

9.7.15 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*|)

Command Mode

Privileged EXEC

Parameter	Parameter Description	Parameter Value
GROUP-ID	Multi-link group ID	1-16

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

9.7.16 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

9.7.17 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

9.7.18 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-multilk-group)#multilink-enhance interface eth-0-1
```

Related Commands

show multi-link group

9.7.19 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-multilk-group)#multilink-enhance receive control-vlan 10 password b interface eth-0-2
```

Related Commands

show multi-link group

9.7.20 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-multilk-group)#multilink-enhance send-interval 20
```

Related Commands

show multi-link group

9.7.21 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-multilk-group)#multilink-enhance timeout 20
```

Related Commands

show multi-link group

9.8 Monitor Link Commands

9.8.1 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

9.8.2 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

9.8.3 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

9.8.4 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

9.8.5 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

9.8.6 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

9.8.7 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

9.8.8 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

9.9 VRRP Commands

9.9.1 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

9.9.2 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

9.9.3 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

9.9.4 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

9.9.5 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

9.9.6 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*advt_interval)+skew_time.when preempt delay time is configured,then master down interval=(3*advt_interval)+skew_time+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

9.9.7 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

9.9.8 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

9.9.9 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
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

9.9.10 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

9.9.11 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

9.9.12 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

9.9.13 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

9.10 Track Commands

9.10.1 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

9.10.2 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

9.10.3 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：

frequency>interval*(packets-per-test-1)+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

9.10.4 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

9.10.5 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

None

9.10.6 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

9.10.7 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

9.10.8 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

9.10.9 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

9.10.10 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

9.10.11 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

9.10.12 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

9.10.13 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

9.10.14 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

9.10.15 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：

(frequency>interval*(packets-per-test-1)+timeout)

Examples

```
Switch#configure terminal
Switch(config)#ip sla monitor 1
Switch(config-ipsla)#packets-per-test 5
```

Related Commands

show ip sla monitor

9.10.16 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

9.10.17 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

9.10.18 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

9.10.19 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

9.10.20 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

9.10.21 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

9.10.22 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	Destionation 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 ipIcmpEcho 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

9.10.23 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

9.10.24 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

9.10.25 vrf

Command Purpose

To use IP SLA operations in VPNs,use vrf in ipsla mode.To remove VPN feathers from IP SLA operations,use the no form of this command.

Command Syntax

vrf *NAME*

no vrf

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

9.11 VARP Commands

9.11.1 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

9.11.2 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

10 Device Management Commands

10.1 STM Commands

10.1.1 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|vlan|ipv4|ipv6)

no stm prefer

Parameter	Parameter Description	Parameter Value
default	Provide balance to all features	-
vlan	Provide maximum system utilization for VLANs.This profile maximizes system memory for use as a Layer 2 switch	-
ipv4	Provide maximum system utilization for unicast routing.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 ipv4
Switch(config)#exit
Switch#reload
```

Related Commands

show stm prefer

10.1.2 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|vlan|ipv4|ipv6)

no stm prefer

Parameter	Parameter Description	Parameter Value
default	Provide balance to all features	-
vlan	Provide maximum system utilization for VLANs.This profile maximizes system memory for use as a Layer 2 switch	-
ipv4	Provide maximum system utilization for unicast routing.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
The selected profile optimizes the resources in
the switch to make balance entry number among
route,mac related tables.

number of Ethernet features:
VLAN number:4094
VLAN forwarding instances:4094
Ucast MAC addresses:32768
Mcast MAC addresses:2048
Blackhole MAC addresses:64
Max applied VLAN mapping:1024
number of OAM features:
```

```
BFD sessions:128
CFM local&remote MEPs:1000
CFM Ethernet Locked Signal:48
G.8031 groups:64
G.8032 rings:32
number of VLAN class rules:
MAC based VLAN classification:256
IPv4 based VLAN classification:512
IPv6 based VLAN classification:256
number of Dot1x Mac entry:
DOT1X MAC BASED:256
number of IP unicast routing:
IPv4 host routes:3072
Indirect IPv4 routes:6144
IPv4 ECMP groups:16
IPv4 policy based routes:32
IPv6 host routes:1024
Indirect IPv6 routes:2048
IPv6 ECMP groups:14
IP Tunnel Peers:8
number of IP multicast routing:
IPv4 Mcast routes:511
IPv4 Mcast total members:1533
IPv6 Mcast routes:127
IPv6 Mcast total members:381
number of Security features:
IPv4 source guard entries:1024
IPv4 ACL/QOS flow entries:831
IPv6 ACL/QOS flow entries:127
```

Related Commands

stm prefer

10.2 Syslog Commands

10.2.1 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

10.2.2 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

10.2.3 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

10.2.4 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 inofrmation.

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

10.2.5 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

10.2.6 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

10.2.7 logging merge

Command Purpose

To enable the logging mergence,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 SIZE	Set fifo size.The range is 100 to 10240,default value is 1024	100-10240
timeout SECONDS	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

10.2.8 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

10.2.9 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

10.2.10 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

10.2.11 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

10.2.12 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

10.2.13 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 sytem	-
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	-
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

10.2.14 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

10.2.15 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

10.2.16 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

10.2.17 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

10.3 Mirror Commands

10.3.1 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

10.3.2 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

10.3.3 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

10.3.4 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

10.3.5 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
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)#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

10.3.6 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

10.3.7 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

10.3.8 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

10.3.9 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(unsupport 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

10.3.10 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

10.3.11 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

10.3.12 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

10.3.13 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

10.3.14 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 captrue	-

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

10.3.15 monitor cpu capture strategy

Command Purpose

Use this command to set the trategy 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

10.3.16 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

10.3.17 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>)

10.3.18 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>

10.3.19 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)

10.4 Device Management Commands

10.4.1 temperature

Command Purpose

To specify the system temperature monitor threshold.

Command Syntax

termperature LOW HIGH CRITICAL

no termperature

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
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

10.4.2 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

10.4.3 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 uImage.r
```

Related Commands

None

10.4.4 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
Port(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
Port(Volts)(Volts)(Volts)(Volts)(Volts)
--------------------------------------------------------------------------------------------------
eth-1-2 3.32 3.80 3.70 2.90 2.80
--------------------------------------------------------------------------------------------------------
High Alarm High Warn Low Warn Low Alarm
Current Threshold Threshold Threshold Threshold
Port(milliamperes)(mA)(mA)(mA)(mA)
--------------------------------------------------------------------------------------------------
eth-1-2 6.41 20.00 18.00 1.00 0.50
--------------------------------------------------------------------------------------------------------
Optical High Alarm High Warn Low Warn Low Alarm
Transmit Power Threshold Threshold Threshold Threshold
Port(dBm)(dBm)(dBm)(dBm)(dBm)
--------------------------------------------------------------------------------------------------
eth-1-2-2.41 2.01 1.00-6.99-7.96
--------------------------------------------------------------------------------------------------------
Optical High Alarm High Warn Low Warn Low Alarm
Receive Power Threshold Threshold Threshold Threshold
Port(dBm)(dBm)(dBm)(dBm)(dBm)
--------------------------------------------------------------------------------------------------
eth-1-2-12-1.00 0.00-19.00-20.00
--------------------------------------------------------------------------------------------------------
```

Related Commands

None

10.4.5 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

10.4.6 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
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

Reboot Type	Description
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

10.5 Bootrom Commands

10.5.1 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

Bootrom 3.0.0(Development build)(Build time:Apr 13 2011-15:31:37)
```

Related Commands

None

10.5.2 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 form 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

10.5.3 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

10.5.4 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

stderr=serial
ipaddr=10.10.29.48
serverip=10.10.29.160
.
Environment size:818/2044 bytes
```

Related Commands

setenv

10.5.5 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

10.5.6 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

10.5.7 ls

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:>ls

Scanning JFFS2 FS:.done
drwxr-xr-x 0 Thu Jan 01 00:00:04 1970 log
drwxr-xr-x 0 Thu Jan 01 00:00:04 1970 boot
drwxr-xr-x 0 Thu Jan 01 00:00:04 1970 conf
-rw-------144 Thu Jan 13 19:51:01 2000 dhcpsnooping
```

Related Commands

None

10.5.8 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

10.5.9 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

10.5.10 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

10.5.11 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

10.5.12 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

10.6 Bootup Diagnostic Commands

10.6.1 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

10.6.2 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

10.6.3 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

10.7 SmartConfig Commands

10.7.1 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

10.7.2 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

11 Network Management Commands

11.1 Network Diagnosis Commands

11.1.1 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

Parameter	Parameter Description	Parameter Value
-f	specify the Don't Fragment flag in packet	-
-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	0-100 second,0 stands for continuous waiting

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

11.1.2 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

11.2 NTP Commands

11.2.1 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

11.2.2 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 enables NTP authentication:

```
Switch#configure terminal
Switch(config)#ntp authentication enable
```

Related Commands

show ntp

11.2.3 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

11.2.4 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

11.2.5 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

11.2.6 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

11.2.7 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

11.2.8 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

11.2.9 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

Parameter	Parameter Description	Parameter Value
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

11.2.10 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

11.2.11 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

11.2.12 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

11.2.13 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

11.2.14 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

11.2.15 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,-outlyer
```

Related Commands

show ntp status

11.2.16 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

11.2.17 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

11.2.18 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

11.2.19 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

11.2.20 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

11.2.21 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

11.3 Phy Loopback Commands

11.3.1 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

11.3.2 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 flied 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

11.3.3 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

11.3.4 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

11.3.5 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
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

11.3.6 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

11.3.7 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

11.3.8 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

11.3.9 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

11.3.10 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

11.3.11 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

11.3.12 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

11.4 RMON Commands

11.4.1 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

11.4.2 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
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

11.4.3 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 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

11.4.4 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

11.4.5 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

11.4.6 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

11.4.7 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

11.4.8 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

11.4.9 rmon clear counters

Command Purpose

Use this command to clear rmon counters.

Command Syntax

rmon clear counters

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

11.4.10 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

11.5 SNMP Commands

11.5.1 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

11.5.2 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 strin	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

11.5.3 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

11.5.4 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

11.5.5 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

11.5.6 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

11.5.7 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

11.5.8 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@exampledomain.com
```

Related Commands

snmp-server system-location

11.5.9 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

11.5.10 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 15000 millisecond	1-1800000 millisecond
retries number	(Optional)The retry time, the default value is 3	0-10
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

11.5.11 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

11.5.12 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/synce/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

11.5.13 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

11.5.14 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 *COMMUINTY*(udpport *UDP_PORT*|)

no snmp-server trap target-address(mgmt-if|vrf *VRF_NAME*|)(*IPV4_ADDR*|*IPV6_ADDR*)community *COMMUINTY*(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
COMMUINTY	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

11.5.15 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 *COMMUINTY*(udpport *UDP_PORT*|)

no snmp-server inform target-address(mgmt-if|vrf *VRF_NAME*|)(*IPV4_ADDR*|*IPV6_ADDR*)community *COMMUINTY*(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
COMMUINTY	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

11.5.16 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

11.5.17 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

Parameter	Parameter Description	Parameter Value
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

11.5.18 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

11.5.19 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

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	-

Parameter	Parameter Description	Parameter Value
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	-

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

11.5.20 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

11.5.21 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

11.5.22 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

11.5.23 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

11.5.24 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

11.5.25 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 00000009020000000c025808 as the local engineID:

```
Switch#show snmp-server engineID

Engine ID:00000009020000000c025808
```

Related Commands

snmp-server engineID

11.5.26 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

11.5.27 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

11.5.28 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

11.5.29 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

11.5.30 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

EnginedID:01234567890123456789
User Name:user1
Auth Protocol:md5
priv Protocol:des
Storage Type:nonvolatile
Row status:active
```

Related Commands

snmp-server usm-user

11.5.31 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

11.5.32 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

11.6 SFLOW Commands

11.6.1 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

11.6.2 sflow agent

Command Purpose

Use this command to configure sFlow agent.

Command Syntax

sflow agent(ip *IPV4_ADDR*|ipv6 ipv6-addres)

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

11.6.3 sflow collector

Command Purpose

Use this command to configure sFlow collector.

Command Syntax

sflow collector(*IPV4_ADDR*|ipv6-addres)(*UDP_PORT*|)

no sflow collector(*IPV4_ADDR*|ipv6-addres)(<*UDP_PORT*|)

Parameter	Parameter Description	Parameter Value
IPV4_ADDR	Collector IPv4 address	IPv4 Address
IPV6_ADDR	Collector IPv6 address	IPv6 Address

Parameter	Parameter Description	Parameter Value
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

11.6.4 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

11.6.5 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

11.6.6 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

11.6.7 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

11.6.8 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:
Flow-Sample Flow-Sample
Port Counter Flow Direction Rate
-------------------------------------------------------
eth-0-1 Disable Enable Input 8192
```

Related Commands

sflow enable

sflow collector

11.7 LLDP Commands

11.7.1 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)

11.7.2 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)

11.7.3 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(intface)

11.7.4 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)

11.7.5 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/vlan/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 themare not be configured,system should use the loopbackinterface,management interface,other interface or system MAC address according descend 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)

11.7.6 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)

11.7.7 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)

11.7.8 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)

11.7.9 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<=tx-delay<=((0.25)*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(global)

lldp enable(interface)

11.7.10 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	-
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)

11.7.11 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|all}

no lldp tlv 8021-org-specific{port-vlan|protocol-vlan|vlan-name|protocol-id|link-aggregation|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	-
all	Select All IEEE 802.1 tlvs,exclude Link Aggregation Tlv	-

Command Mode

Interface Configuration

Default

All IEEE 802.1 tlvs 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)

11.7.12 lldp tlv 8021-org-specific vlan-name-value

Command Purpose

To configure the value forVLAN NAME TLV in the IEEE 802.1 tlvs,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)

11.7.13 lldp tlv 8023-org-specific

Command Purpose

To select the IEEE 802.3 tlvs 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 tlvs	-

Command Mode

Interface Configuration

Default

All IEEE 802.3 tlvs 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)

11.7.14 lldp tlv med

Command Purpose

To select the MED tlvs 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 tlvs is selected,exclude Location Identification Tlv.

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)

11.7.15 lldp 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)

11.7.16 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

11.7.17 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	-

Parameter	Parameter Description	Parameter Value
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
Power Via 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

11.7.18 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)

11.7.19 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

11.7.20 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

12 VPN Commands

12.1 GRE TUNNEL Commands

12.1.1 interface

Command Purpose

Using this command to create a new tunnel interface.Use the no form of this command to destroy the tunnel interface.

Command Syntax

interface tunnel *TUNNEL_ID*

no interface tunnel *TUNNEL_ID*

Parameter	Parameter Description	Parameter Value
TUNNEL_ID	tunnel id	0-1023

Command Mode

Global Configuration

Default

None

Usage

It just creates an interface structure,and then the tunnel interface can not be used before it is configured the mode.

Examples

This example shows how to create a tunnel interface.:

```
Switch#configure terminal
Switch(config)#interface tunnel 1
```

Related Commands

show interface tunnel

12.1.2 tunnel mode gre

Command Purpose

This cammad is used for specifying the IPv4 transition tunnel protocol of gre,and the no form of this command can unset the tunnel protocol.

Command Syntax

tunnel mode gre

no tunnel mode

Parameter	Parameter Description	Parameter Value
gre	The gre tunnel is only supported in IPv4 network and encaped with IPv4 header.	-

Command Mode

Interface Configuration

Default

None

Usage

When configure the tunnel mode with gre,and then it is required configure tunnel source and tunnel destination manually.

Examples

This example shows how to configure the tunnel with gre protocol:

```
Switch#configure terminal
Switch(config)#interface tunnel 1
Switch(config-if)#tunnel mode gre
```

Related Commands

tunnel source

tunnel destination

12.1.3 tunnel source

Command Purpose

This command is used 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,like routed port,vlan interface,loopback..	Support physical/aggregation/loopback/vlan ports

Command Mode

Interface Configuration

Default

None

Usage

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 gre

tunnel destination

12.1.4 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

None

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 gre

12.1.5 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)

Parameter	Parameter Description	Parameter Value
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

12.1.6 tunnel gre key

Command Purpose

Use this command to set the key of gre tunnel.Use the no form of this command to unset the key of gre tunnel.

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

Gre key is taken advantage of certification of packet and provides the security of gre tunnel.Gre key can support 32bits,but can not support to set 0.

Examples

This example shows how to set gre key.:

```
Switch#configure terminal
Switch(config)#interface tunnel 1
Switch(config-if)#tunnel gre key 666
```

Related Commands

tunnel source

12.1.7 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 inheriting 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

show interface tunnel

interface

12.1.8 keepalive

Command Purpose

Use this command to enable function of keepalive,it is used for checking whether gre tunnel peers is up or reachable.

Command Syntax

keepalive PERIOD_VALUE RETRY_VALUE

no keepalive

Parameter	Parameter Description	Parameter Value
PERIOD_VALUE	Interval period	1-32767
RETRY_VALUE	timeout and retry	1-255

Command Mode

Interface Configuration

Default

period_value:10s

retry_value:3

Usage

Only when the gre tunnel is in the state of up or keepalive down,then the keepalive packets can be sent out through the network port.

Examples

This example shows how to enable the keepalive function with period value 10s and retry times 5:

```
Switch#configure terminal
Switch(config)#interface tunnel 1
Switch(config-if)#keepalive 10 5
```

Related Commands

no keepalive

12.1.9 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 tunnel 1

Interface tunnel1
Interface current state:UP
Hardware is Tunnel
Index 8193,Metric 1,Encapsulation TUNNEL
VRF binding:not bound
Internet primary address:
1.1.1.1/24 pointopoint 1.1.1.255
Tunnel protocol/transport GRE/IP,Status Valid
Tunnel source 192.192.168.1(eth-0-10),destination 10.10.10.10
Tunnel DSCP inherit,Tunnel TTL 255
Tunnel transport MTU 1476 bytes
Tunnel GRE key enable:100
Tunnel GRE keepalive enable,Send period:5,Retry times:3
0 packets input,0 bytes
0 packets output,0 bytes
```

Related Commands

show resource tunnel

12.1.10 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 tunnel resource

Tunnel
Resource Used Capability
============================================================
Peers 0 8
DUT1#
```

Related Commands

None

12.1.11 show tunnel keepalive statistics

Command Purpose

Use this command to display the statistics of gre tunnel keepalive.

Command Syntax

show tunnel keepalive statistics(|interface tunnel *TUNNEL_ID*)

Parameter	Parameter Description	Parameter Value
TUNNEL_ID	tunnel id	0-1023

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example displays the statistics of gre tunnel keepalive.:

```
Switch#show tunnel keepalive statistics

Name Status Keepalive Out_ka_pkt In_ka_pkt TunnelUp TunnelDown
--------------------------------------------------------------------------------
DUT1#
```

Related Commands

clear tunnel keepalive statistics

12.1.12 clear tunnel keepalive statistics

Command Purpose

Use this command to clear the statistics of gre tunnel keepalive.

Command Syntax

clear tunnel keepalive statistics(all|interface tunnel *TUNNEL_ID*)

Parameter	Parameter Description	Parameter Value
TUNNEL_ID	tunnel id	0-1023

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example clears the statistics of gre tunnel keepalive.:

```
Switch#clear tunnel keepalive statistics all
```

Related Commands

show tunnel keepalive statistics

12.1.13 clear tunnel statistics

Command Purpose

Use this command to clear the statistics of tunnel include input and output.

Command Syntax

clear tunnel statistics(all|interface tunnel *TUNNEL_ID*)

Parameter	Parameter Description	Parameter Value
TUNNEL_ID	tunnel id	0-1023

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example clears the statistics of tunnel include input and output.:

```
Switch#clear tunnel statistics all
```

Related Commands

show interface tunnel id

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.

Copyright © 2009-2022 FS.COM All Rights Reserved.